

Secret-Key Agreement Capacity over Reciprocal Fading Channels: A Separation Approach

Ashish Khisti

Dept. of Electrical and Computer Engineering

University of Toronto

Toronto, ON, Canada

Email: akhisti@comm.utoronto.ca

Abstract—Fundamental limits of secret-key agreement over reciprocal wireless channels are investigated. We consider a two-way block-fading channel where the channel gains in the forward and reverse links between the legitimate terminals are correlated. The channel gains between the legitimate terminals are not revealed to any terminal, whereas the channel gains of the eavesdropper are revealed to the eavesdropper. We propose a two-phase transmission scheme, that reserves a certain portion of each coherence block for channel estimation, and the remainder of the coherence block for correlated source generation. The resulting secret-key involves contributions of both channel sequences and source sequences, with the contribution of the latter becoming dominant as the coherence period increases. We also establish an upper bound on the secret-key capacity, which has a form structurally similar to the lower bound. Our upper and lower bounds coincide in the limit of high signal-to-noise-ratio (SNR) and large coherence period, thus establishing the secret-key agreement capacity in this asymptotic regime. Numerical results indicate that the proposed scheme achieves significant gains over training-only schemes, even for moderate SNR and small coherence periods, thus implying the necessity of randomness-sharing in practical secret-key generation systems.

I. INTRODUCTION

Physical layer can provide a valuable resource for enhancing security and confidentiality of wireless communication systems. One promising method that has received a significant interest in recent years (see e.g., [1]–[20] and the references therein) is the generation of a shared secret key using channel reciprocity. When the terminals use identical carrier frequencies, a physical reciprocity [21] exists between uplink and downlink channels, which provides a natural mechanism for key exchange. The terminals first transmit training signals to estimate the underlying channel gains, then agree on a common sequence using error correction, and finally distill a shared secret-key from this common sequence. A number of experimental testbeds already demonstrate practical viability of such methods. See e.g., [13], [18]–[20].

Despite this growing interest, information theoretic limits of secret-key agreement over wireless channels have not received much attention. Consider a block-fading channel where the channel gains are sampled once every coherence period and

remain constant during the coherence block. Clearly, channel reciprocity alone achieves a rate that vanishes as the coherence period increases. What form of signalling within each coherence block maximizes the secret-key rate? To our knowledge, only a recent paper [22] considers this question. The authors consider a separation based scheme. A portion of each coherence block is reserved for transmission of pilot symbols to estimate the channel coefficients. The remainder of the coherence block is used for transmission of a *confidential-message*. Unfortunately the authors observe that one cannot separately tune the two phases. Any rate/power adaptation done during the message transmission phase, leaks information about the channel gains to an eavesdropper and in turn reduce the contribution from reciprocity. As such the wiretap code for confidential message transmission proposed in [22] does not involve any rate or power adaptation. It achieves a non-zero rate only if we impose that the eavesdropper's channel on average be weaker than the legitimate receiver's channel. If this condition is not satisfied, the secret-key rate achieved in [22] reduces to the rate achieved using a training only scheme and vanishes to zero as the coherence period becomes large.

In the present paper we too consider a separation based scheme, but substitute the confidential-message transmission phase with a different communication strategy — *randomness sharing*. Following the training phase, in each coherence block the terminals exchange i.i.d. random variables to generate correlated source sequences between the terminals. No power allocation is performed during this phase, yet it results in a positive secret-key rate even when the eavesdropper's channel is on average stronger than the legitimate receiver's channel. We note that the *randomness sharing* scheme for secret-key generation has been investigated in several previous works (see e.g., [23]–[28] and references therein). However to the author's knowledge, the present paper appears to be the first attempt that studies randomness sharing, in conjunction with training techniques, in non-coherent wireless channels. Furthermore our proposed scheme has several appealing features. First it achieves a rate that does not vanish in the large coherence-period limit, thus making it attractive in this practically relevant regime. Secondly our proposed separation scheme is asymptotically optimal among all signalling schemes in the two-way fading channel. In particular, we also establish

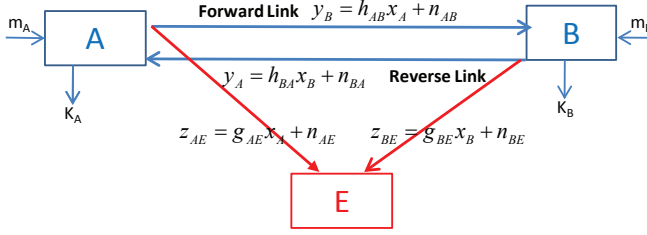


Fig. 1. Problem Setup. There are two legitimate terminals and one eavesdropper terminal. The legitimate terminals A and B are required to agree on a common secret-key. The fading gains h_{AB} and h_{BA} are not revealed to any terminals, whereas the g_{AE} and g_{BE} are revealed to the eavesdropper.

an upper bound on the secret-key agreement capacity in the proposed setup. The upper bound expression is structurally similar to the lower bound expression and furthermore the difference between our upper and lower bound vanishes to zero in the limit of large coherence period and high signal-to-noise-ratio, thus establishing an asymptotic capacity result. Numerical results indicate that even for moderate SNR and relatively small coherence periods the gains resulting from randomness sharing are significant over training-only schemes.

Our proposed model also differs from reference [22] in that we only assume *imperfect* reciprocity in uplink and downlink channels i.e., we assume that the channel gains in uplink and downlink are correlated, but not identical. In general achieving perfect channel reciprocity in baseband is challenging because different terminals use different I/Q mixers, amplifiers and path lengths in the RF chains. While closed-loop calibration can be performed (see e.g. [29], [30]), such methods can become challenging if the calibration needs to be done in the open air. Hence we believe that our assumption of imperfect reciprocity may perhaps be more realistic in practice. Nevertheless we also note that our coding technique can also be applied to the case of perfect reciprocity, and improves upon the message transmission scheme [22].

In other related works, an information theoretic framework for secure communication was pioneered by Shannon [31]. The problem of secret-key generation from common randomness between two legitimate terminals was introduced in [23], [24]. The setup considered in these papers involves one-way communication channel models and a public-discussion channel. In followup works, secret-key agreement capacity over one-way fading channels with a noiseless public feedback link have been studied in e.g. [32]–[36]. References [37]–[39] study secret-key agreement over a channel with two-sided state sequence, which has application to fading channels. However these works do not incorporate the cost of acquiring channel state information which is of critical importance in the proposed setup.

II. SYSTEM MODEL AND MAIN RESULTS

As illustrated in Fig. 1, we consider a setup with two legitimate terminals A and B and one eavesdropper E . The terminals A and B communicate over a two-way non-coherent wireless channel:

$$y_B(t) = h_{AB}(t)x_A(t) + n_B(t), \quad y_A(t) = h_{BA}(t)x_B(t) + n_A(t), \quad (1)$$

$$z_{AE}(t) = g_{AE}(t)x_A(t) + n_{AE}(t), \quad z_{BE}(t) = g_{BE}(t)x_B(t) + n_{BE}(t) \quad (2)$$

where $t \in \{1, \dots, N\}$ denotes the time index, $y_A(t)$ and $y_B(t)$ denote the output symbols at terminals A and B and $\{z_{AE}(t), z_{BE}(t)\}$ denote the output symbols at terminal E . The input symbols generated by terminals A and B at time t are denoted by $x_A(t)$ and $x_B(t)$ respectively and are required to satisfy the average power constraints:

$$\frac{1}{N} \sum_{t=1}^N E[|x_A(t)|^2] \leq P, \quad \frac{1}{N} \sum_{t=1}^N E[|x_B(t)|^2] \leq P$$

The channel gains $(h_{AB}, h_{BA}, g_{AE}, g_{BE})$ are drawn from a distribution $p(h_{AB}, h_{BA})p(g_{AE}, g_{BE})$ once every T consecutive symbols and stay constant over this period i.e., the channel gains remain constant in the interval $t \in [iT + 1, (i+1)T]$ for $i = 0, 1, \dots, \frac{N}{T} - 1$. We assume that the channel gains $h_{AB}(t)$ and $h_{BA}(t)$ are not revealed to any of the terminals apriori, whereas the channel gains $(g_{AE}(t), g_{BE}(t))$ are revealed to the eavesdropper terminal. The additive noise variables are drawn from an i.i.d. $\mathcal{CN}(0, 1)$ distribution. When computing the achievable rates, for convenience, we will assume that the channel gains are all drawn from the Gaussian $\mathcal{CN}(0, 1)$ distribution, although our results are not tied to this assumption.

Remark 1: While we assume that the channel gains of the eavesdropper are independent of (h_{AB}, h_{BA}) , our results naturally extend to the case when the channel gains are drawn from a joint distribution $p(h_{AB}, h_{BA}, g_{AE}, g_{BE})$. Also note that the eavesdropper observes the transmission from the two terminals A and B over non-interfering links. An eavesdropper who observes a superposition of the two signals can only be weaker than the proposed eavesdropper.

Definition 1 (Secret-Key Capacity): A feasible secret-key generation protocol is defined as follows. Terminals A and B sample independent random variables m_A and m_B from a product distribution $p(m_A)p(m_B)$. At time t , terminals A and B generate the symbols $x_A(t) = f_A(m_A, y_A^{t-1})$ and $x_B(t) = f_B(m_B, y_B^{t-1})$. At the end of N channel uses, the terminals A and B generate secret keys k_A and k_B respectively using the functions $k_A = \mathcal{K}_A(y_A^N, m_A)$ and $k_B = \mathcal{K}_B(y_B^N, m_B)$. We require that $\Pr(k_A \neq k_B) \leq \varepsilon_N$ and furthermore $\frac{1}{N} I(k_A; \mathbf{z}^N, \mathbf{g}^K) \leq \varepsilon_N$ for some sequence ε_N that goes to zero as $N \rightarrow \infty$. The largest achievable rate $R = \frac{1}{N} H(k_A)$ is denoted as the *secret-key capacity*. \square

As our main result, we establish upper and lower bounds on the secret-key capacity for the two-way non-coherent channel model.



Fig. 2. Separation-based approach for secret-key generation. In each coherence block of length T symbols, the first symbol is dedicated to training and a power P_1 is used i.e., $x_A(iT+1) = x_B(iT+1) = \sqrt{P_1}$. The remaining $T-1$ symbols are used for randomness generation. Each symbol is sampled i.i.d. $\mathcal{CN}(0, P_2)$ in this phase.

A. Upper Bound

Theorem 1: An upper-bound on the secret-key capacity of the two-way non-coherent fading channel is,

$$C \leq R^+ = \frac{1}{T} I(h_{AB}; h_{BA}) + \max_{\{P(h_{AB})\} \in \mathcal{P}_{AB}} \{I(y_B; x_A | h_{AB}, z_{AE}, g_{AE})\} + \max_{\{P(h_{BA})\} \in \mathcal{P}_{BA}} \{I(y_A; x_B | h_{BA}, z_{BE}, g_{BE})\}, \quad (3)$$

where the above expression is evaluated for

$$x_A \sim \mathcal{CN}(0, P(h_{AB})), \quad x_B \sim \mathcal{CN}(0, P(h_{BA})),$$

and the set \mathcal{P}_{AB} is the set of all non-negative power allocation functions $P(h_{AB})$ that satisfy the average power constraint $E[P(h_{AB})] \leq P$ and the set \mathcal{P}_{BA} is defined similarly.

Remark 2: The upper bound expression in Theorem 1 has a natural interpretation. The term $\frac{1}{T} I(h_{AB}; h_{BA})$ is the contribution arising from reciprocal channel gains. The second term is the secret key rate achieved over a one way fading channel

$$y_B = h_{AB}x_A + n_B, \quad z_{AE} = g_{AE}x_A + n_{AE} \quad (4)$$

and a public discussion channel in the reverse link, when the fading chain h_{AB} is revealed to all the terminals and the channel gain g_{AE} is revealed to the eavesdropper. Likewise the third term is the contribution arising from the one-way fading channel in the reverse link. The upper bound expression (3) indicates that the contribution of these three terms is additive. \square

The proof of Theorem 1 is provided in section III.

B. Lower Bound - Public Discussion

Our proposed coding scheme involves a separation based approach. As shown in Fig. 2, the first symbol in each coherence block is reserved for sending a training symbol and a total power of P_1 is used in this phase. This allows the terminals B and A to generate linear minimum mean squared error estimates of the channel gains h_{AB} and h_{BA} respectively i.e.,

$$\hat{h}_{AB} = \alpha h_{AB} + e_{AB} \quad (5)$$

$$\hat{h}_{BA} = \alpha h_{BA} + e_{BA}, \quad (6)$$

where $\alpha = \frac{P_1}{P_1+1}$ is the estimation coefficient, and e_{AB} and e_{BA} both have the distribution $\mathcal{CN}(0, \alpha(1-\alpha))$ and are independent of the channel gains h_{AB} and h_{BA} respectively.

For the reminder of coherence block, both the terminals transmit i.i.d. symbols from $\mathcal{CN}(0, P_2)$ to generate correlated source sequences i.e., in coherence period i each component of the vector $\bar{x}_A(i) \in \mathbb{C}^{T-1}$ is generated i.i.d. $\mathcal{CN}(0, P_2)$ and similarly each component of the vector $\bar{x}_B(i)$ is i.i.d. $\mathcal{CN}(0, P_2)$. The corresponding received vectors are given by

$$\bar{y}_A(i) = h_{BA}(i)\bar{x}_B(i) + \bar{n}_{BA}(i), \quad \bar{y}_B(i) = h_{AB}(i)\bar{x}_A(i) + \bar{n}_{AB}(i). \quad (7)$$

At the end of K such coherence blocks, as indicated in Table I, terminal A has access to $(\hat{h}_{BA}^K, \bar{x}_A^K, \bar{y}_A^K)$ whereas terminal B has access to $(\hat{h}_{AB}^K, \bar{x}_B^K, \bar{y}_B^K)$. The eavesdropper observes $(g_{AE}^K, g_{BE}^K, \bar{z}_{AE}^K, \bar{z}_{BE}^K)$.

TABLE I
CORRELATED SOURCE AND CHANNEL SEQUENCES AT THE TERMINALS

Sequence/Terminal	A	B	E
Channel Sequence	\hat{h}_{BA}^K	\hat{h}_{AB}^K	(g_{AE}^K, g_{BE}^K)
Source Sequence - I	\bar{x}_A^K	\bar{y}_B^K	\bar{z}_{AE}^K
Source Sequence - II	\bar{y}_A^K	\bar{x}_B^K	\bar{z}_{BE}^K

These correlated sequences are in turn used to generate a common secret-key by exchanging suitable public messages in the reconciliation phase [23], [24]. As indicated, in this section we assume that these public-messages for secret-key generation are transmitted over an external public discussion channel. The resulting rate-expression is simpler and has a form that can be immediately compared with the upper bound. Subsequently we will remove this assumption and consider the transmission of public messages directly over the wireless channel.

Theorem 2: An achievable secret-key rate when an additional public discussion channel of arbitrarily high rate is available communication is given by

$$R_{PD}^- = \frac{1}{T} I(\hat{h}_{AB}; \hat{h}_{BA}) + \frac{T-1}{T} \left\{ I(y_B; x_A, \hat{h}_{AB}, \hat{h}_{BA}) - I(y_B; z_{AE}, g_{AE}, h_{AB}) \right\} + \frac{T-1}{T} \left\{ I(y_A; x_B, \hat{h}_{BA}, \hat{h}_{AB}) - I(y_A; z_{BE}, g_{BE}, h_{BA}) \right\}, \quad (8)$$

where we evaluate the expression for $x_A \sim \mathcal{CN}(0, P_2)$ and $x_B \sim \mathcal{CN}(0, P_2)$ and \hat{h}_{AB} and \hat{h}_{BA} are specified in (5) and (6) respectively and P_1 and P_2 are non-negative and satisfy the relation

$$P_1 + (T-1)P_2 \leq TP. \quad (9)$$

A proof of Theorem 2 is sketched in Section IV.

Remark 3: The lower bound expression (8) differs in the following respects from the upper bound expression (3): (i) the channel gains h_{AB} and h_{BA} in the first term are replaced by their estimates \hat{h}_{AB} and \hat{h}_{BA} respectively; (ii) the second and third terms are scaled by a factor of $(1 - \frac{1}{T})$; (iii) in computing the second and third terms, we assume that the legitimate receivers have access to the channel estimates whereas the eavesdropper has access to perfect channel states;

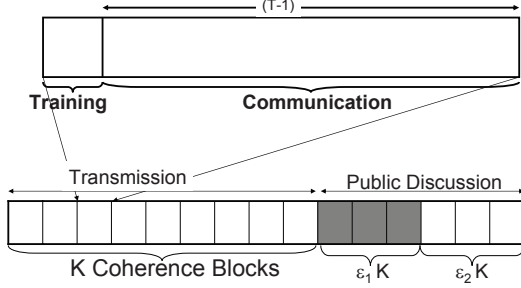


Fig. 3. Extension of the proposed coding scheme in absence of public discussion. A total of K coherence blocks are used for training and source emulation. Thereafter a total of $\varepsilon_1 K$ coherence blocks are used for transmission of the public message associated with the channel sequences and another $\varepsilon_2 K$ coherence blocks are used for the transmission of the public message associated with the source sequences.

(iv) power allocation across the channel gains is not performed in the lower bound expression.

An explicit evaluation of the lower bound when that the channel gains h_{AB} and h_{BA} are jointly Gaussian, zero mean random variables with a cross-correlation of ρ is as follows.

Proposition 1: An achievable secret-key rate when terminals A and B have access to a public discussion channel is given by:

$$R_{PD}^- = \frac{1}{T} R_{P,T}^- + \frac{T-1}{T} (R_{P,AB}^- + R_{P,BA}^-) \quad (10)$$

where the expressions for $R_{P,T}^-$, $R_{P,AB}^-$ and $R_{P,BA}^-$ are given by:

$$R_{P,T}^- = -\log(1 - \alpha^2 \rho^2) \quad (11)$$

$$R_{P,AB}^- = E \left[\log \left(1 + \frac{P_2 |h_{AB}|^2}{1 + P_2 |g_{AE}|^2} \right) \right] - \log \left(1 + \frac{P_2}{1 + P_1} \right) \quad (12)$$

$$R_{P,BA}^- = E \left[\log \left(1 + \frac{P_2 |h_{BA}|^2}{1 + P_2 |g_{BE}|^2} \right) \right] - \log \left(1 + \frac{P_2}{1 + P_1} \right). \quad (13)$$

and $\alpha = \frac{P_1}{1+P_1}$. \square

The proof of Prop. 1 is provided in section IV-D.

C. Lower Bound - No Discussion

When a separate discussion channel is not available, we use the communication channel for sending the public messages during the key-generation step as illustrated in Fig. 3. We also need to quantize the source sequences to satisfy the rate constraint imposed by the channel.

Theorem 3: An achievable secret-key rate in the absence of public discussion for the two-way reciprocal fading channel is:

$$R^- = \frac{1}{1 + \varepsilon_1 + \varepsilon_2} \left(\frac{1}{T} R_I + \frac{T-1}{T} R_{II} \right). \quad (14)$$

We provide the expressions for R_I and R_{II} below, both of which depend on ε_1 and ε_2 .

$$R_I = I(u_{AB}; \hat{h}_{BA}) + I(u_{BA}; \hat{h}_{AB}) - I(u_{AB}; u_{BA}) \quad (15)$$

where the random variables u_{AB} and u_{BA} satisfy the Markov chain

$$u_{AB} \rightarrow \hat{h}_{AB} \rightarrow \hat{h}_{BA} \rightarrow u_{BA}, \quad (16)$$

and the rate constraints

$$I(u_{AB}; \hat{h}_{AB} | \hat{h}_{BA}) \leq (T-1) \varepsilon_1 R_{NC}(P), \quad (17)$$

$$I(u_{BA}; \hat{h}_{BA} | \hat{h}_{AB}) \leq (T-1) \varepsilon_1 R_{NC}(P), \quad (18)$$

where $R_{NC}(P)$ is an achievable rate for the non-coherent block fading channel (see e.g., [40]).

The rate expression for R_{II} is expressed as $R_{II} = R_{AB}^- + R_{BA}^-$, where

$$R_{AB}^- = I(v_B; x_A, u) - I(v_B; z_{AE}, g_{AE}, h_{AB}), \quad (19)$$

$$R_{BA}^- = I(v_A; x_B, u) - I(v_A; z_{BE}, g_{BE}, h_{BA}) \quad (20)$$

where the random variable $u \triangleq (u_{AB}, u_{BA})$. The random variables v_A and v_B in (20) and (19) satisfy the following Markov Conditions

$$v_A \rightarrow y_A \rightarrow (u, x_B), \quad v_B \rightarrow y_B \rightarrow (u, x_A). \quad (21)$$

as well as the rate constraints:

$$I(v_A; y_A | u, x_B) \leq \varepsilon_2 R_{NC}(P), \quad (22)$$

$$I(v_B; y_B | u, x_A) \leq \varepsilon_2 R_{NC}(P). \quad (23)$$

\square

A proof of Theorem 3 appears in section V.

We further evaluate the rate expression in Theorem 3 for a Gaussian test channel:

$$u_{AB} = \hat{h}_{AB} + q_{AB}, \quad u_{BA} = \hat{h}_{BA} + q_{BA} \quad (24)$$

where $q_{AB}, q_{BA} \sim \mathcal{CN}(0, Q_1)$ are Gaussian random variables independent of all other variables. Similarly we let

$$v_A = y_A + w_A, \quad v_B = y_B + w_B \quad (25)$$

where $w_A, w_B \sim \mathcal{CN}(0, Q_2)$ are Gaussian random variables independent of all other variables.

Proposition 2: An achievable secret-key rate in the absence of public discussion for the two-way reciprocal fading channel is given by:

$$R^- = \frac{1}{1 + \varepsilon_1 + \varepsilon_2} \left\{ \frac{1}{T} R_I(\varepsilon_1, P_1) + \frac{T-1}{T} R_{II}(\varepsilon_2, P_2) \right\} \quad (26)$$

where P_1 and P_2 are non-negative and satisfy (9) and ε_1 and ε_2 are non-negative constants that will be specified in the sequel. The rate expressions R_I and R_{II} are as follows.

$$R_I(\varepsilon_1, P_1) = \left\{ -2 \log \left(1 - \frac{\alpha^2 \rho^2}{1 + \frac{Q_1}{\alpha}} \right) + \log \left(1 - \frac{\alpha^2 \rho^2}{\left(1 + \frac{Q_1}{\alpha} \right)^2} \right) \right\} \quad (27)$$

where $\alpha = \frac{P_1}{1+P_1}$ and Q_1 satisfies

$$\log \left(1 + \frac{\alpha(1 - \alpha^2 \rho^2)}{Q_1} \right) \leq \varepsilon_1 T R_{NC}(P). \quad (28)$$

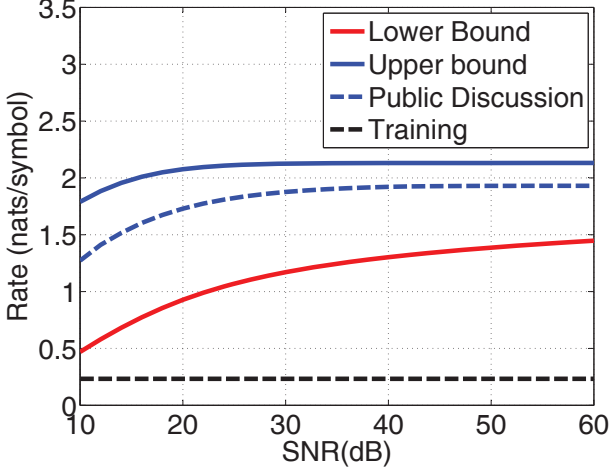


Fig. 4. Bounds on the SK capacity as a function of SNR for a coherence period of $T = 10$.

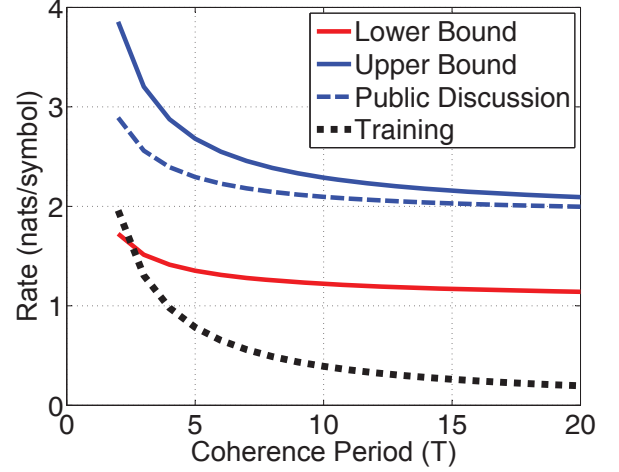


Fig. 5. Bounds on the SK capacity as a function of coherence period for SNR = 30dB.

The expression for R_{II} satisfies

$$R_{II}(\varepsilon_2, P_2) = \left\{ R_{AB}^-(\varepsilon_2, P_2) + R_{BA}^-(\varepsilon_2, P_2) \right\}, \quad (29)$$

$$R_{AB}^-(\varepsilon_2, P_2) = E \left[\log \left(1 + \frac{P_2 |h_{AB}|^2}{(1 + Q_2)(1 + P_2 |g_{AE}|^2)} \right) \right] - \log \left(\frac{\sigma_{AB}^2 P_2}{1 + Q_2} + 1 \right), \quad (30)$$

$$R_{BA}^-(\varepsilon_2, P_2) = E \left[\log \left(1 + \frac{P_2 |h_{BA}|^2}{(1 + Q_2)(1 + P_2 |g_{BE}|^2)} \right) \right] - \log \left(\frac{\sigma_{BA}^2 P_2}{1 + Q_2} + 1 \right), \quad (31)$$

where

$$\sigma_{AB}^2 = \sigma_{BA}^2 = 1 - \frac{\alpha^2}{Q_1 + \alpha} \quad (32)$$

and Q_2 satisfies

$$\log \left(1 + \frac{\sigma_{AB}^2 P_2 + 1}{Q_2} \right) \leq \varepsilon_2 R_{NC}(P). \quad (33)$$

□

A proof of Prop. 2 appears in section V-H.

Remark 4: The rate achieved in Prop. 2 reduces to the rate achieved using public discussion in Prop. 1 when we take $Q_1 = Q_2 = 0$. In particular when $Q_1 = 0$ note that the expression for R_I in (27) immediately reduces to (10). Furthermore (32) reduces to

$$\sigma_{AB}^2 = \sigma_{BA}^2 = \frac{1}{1 + P_1}. \quad (34)$$

Substituting $Q_2 = 0$, and (34) in (30) and (31) we obtain (12) and (13) respectively. Thus the rate expressions in Prop. 2 are consistent with the expressions in Prop. 1 when quantization (c.f. (24) and (25)) is not introduced.

We also observe that the upper and lower bounds are close in the high signal-to-noise-ratio (SNR) regime.

Corollary 1: In the high SNR regime the upper and lower bounds satisfy the following relation:

$$\lim_{P \rightarrow \infty} R^+(P) - R_{PD}^-(P) = \frac{1}{T} \gamma \quad (35)$$

$$\lim_{P \rightarrow \infty} R^+(P) - R^-(P) = \frac{1}{T} \gamma \quad (36)$$

where R^+ , R_{PD}^- and R^- are given by (3), (10) and (26) respectively and

$$\gamma \triangleq E \left[\log \left(1 + \frac{|h_{AB}|^2}{|g_{AE}|^2} \right) \right] + E \left[\log \left(1 + \frac{|h_{BA}|^2}{|g_{BE}|^2} \right) \right] \quad (37)$$

is a constant that only depends on the distributions $p(h_{AB})p(g_{AE})$ and $p(h_{BA})p(g_{BE})$.

A proof of Corollary 1 appears in section VI.

Numerical Comparison:

Fig. 4 shows the bounds on secret-key capacity as a function of SNR when the coherence period $T = 10$. Fig. 5 shows the bounds as a function of the coherence period T when SNR = 35 dB. In Fig. 4 we fix the correlation coefficient in uplink and downlink gains to $\rho = 0.95$ while in Fig. 5 it is fixed to $\rho = 0.99$.

We make several observations in these plots. The lowermost plot in both figures corresponds to the best rate any training based scheme can achieve i.e.,

$$R_{\text{training}} = -\frac{1}{T} \log(1 - \rho^2) \quad (38)$$

In computing (38) we assume that the legitimate receivers have a genie-aided side information of the respective channel gains and furthermore no overhead arising from the transmission of public messages is considered. In Fig. 4 this rate is SNR independent and in Fig. 5 it decreases to zero as $\frac{1}{T}$.

The upper-most plot in Fig. 4 and Fig. 5 is the upper bound on the secret-key agreement capacity for any scheme. We note that for small values of T the contribution from channel-reciprocity term in (3) is dominant. As T increases

the contribution of this term diminishes and the contribution from the communication channel increases (c.f. (3)).

The remaining two plots are the lower bounds with and without public discussion. The lower bound with public discussion does not involve the overhead of transmitting a public message. For sufficiently high SNR, it approaches the upper bound. The lower bound without public discussion does not come close to the upper in the SNR range of interest. Nevertheless it achieves a much higher rate than the training based schemes.

III. PROOF OF THEOREM 1

In this section we provide a proof of Theorem 1. We assume that the communication is over a total of K coherence blocks and let $N = T \cdot K$ denote the total number of channel uses. Thus the channel state-sequences are of length K whereas the channel input and output sequences are of length N . We use the notation h_{AB}^K to denote the channel state sequence of length K and the notation x_A^N to denote a channel input sequence of length N . For the eavesdropper, we use the notation $\mathbf{z}^N \triangleq (z_{AE}^N, z_{BE}^N)$ and $\mathbf{g}^K \triangleq (g_{AE}^K, g_{BE}^K)$.

From the Fano's inequality and the secrecy constraint we have that

$$NR \leq I(k_A; k_B) - I(k_A; \mathbf{z}^N, \mathbf{g}^K) + 2n\varepsilon_n \quad (39)$$

$$\leq I(k_A; k_B | \mathbf{z}^N, \mathbf{g}^K) + 2n\varepsilon_n \quad (40)$$

where $\varepsilon_n \rightarrow 0$ as $n \rightarrow \infty$. In the following steps the term ε_n will be suppressed. Since $k_A = f_A(m_A, y_A^N)$ and $k_B = f_B(m_B, y_B^N)$, using the data-processing inequality and the chain rule of mutual information, we have:

$$\begin{aligned} NR &\leq I(m_A, h_{BA}^K, y_A^N; m_B, h_{AB}^K, y_B^N | \mathbf{z}^N, \mathbf{g}^K) \\ &= I(m_A, h_{BA}^K, y_A^N; m_B, h_{AB}^K, y_B^{N-1} | \mathbf{z}^N, \mathbf{g}^K) + \\ &\quad I(m_A, h_{BA}^K, y_A^N; y_B(N) | \mathbf{z}^N, \mathbf{g}^K, m_B, h_{AB}^K, y_B^{N-1}) \\ &= I(m_A, h_{BA}^K, y_A^{N-1}; m_B, h_{AB}^K, y_B^{N-1} | \mathbf{z}^N, \mathbf{g}^K) + \\ &\quad I(y_A(N); m_B, h_{AB}^K, y_B^{N-1} | \mathbf{z}^N, \mathbf{g}^K, m_A, h_{BA}^K, y_A^{N-1}) + \\ &\quad I(m_A, h_{BA}^K, y_A^{N-1}; y_B(N) | \mathbf{z}^N, \mathbf{g}^K, m_B, h_{AB}^K, y_B^{N-1}) + \\ &\quad I(y_A(N); y_B(N) | \mathbf{z}^N, \mathbf{g}^K, m_B, h_{AB}^K, y_B^{N-1}, m_A, h_{BA}^K, y_A^{N-1}). \end{aligned} \quad (41)$$

We bound each of the four terms in (41). We show that the following condition holds

$$\begin{aligned} &I(m_A, h_{BA}^K, y_A^{N-1}; m_B, h_{AB}^K, y_B^{N-1} | \mathbf{z}^N, \mathbf{g}^K) \\ &\leq I(m_A, h_{BA}^K, y_A^{N-1}; m_B, h_{AB}^K, y_B^{N-1} | \mathbf{z}^{N-1}, \mathbf{g}^K) \end{aligned} \quad (48)$$

in the steps between (42) and (47) on the top of next page. Note that (45) follows from the fact that $x_A(N)$ is a function of (m_A, y_A^{N-1}) and furthermore $z_{AE}(N)$ is independent of all other random variables given $(x_A(N), g_{AE}(N))$ (c.f. (2)). Eq. (47) similarly follows because $x_B(N)$ is a function of (m_B, y_B^{N-1}) and furthermore $z_{BE}(N)$ is independent of all other random variables given $(x_B(N), g_{BE}(N))$.

Furthermore, since $(y_A(N), z_{BE}(N))$ are independent of all other random variables given $(x_B(N), h_{BA}(N), g_{BE}(N))$ we can show that

$$I(y_A(N); m_B, h_{AB}^K, y_B^{N-1} | \mathbf{z}^N, \mathbf{g}^K, m_A, h_{BA}^K, y_A^{N-1})$$

$$\leq I(y_A(N); x_B(N) | z_{BE}(N), g_{BE}(N), h_{BA}(N)). \quad (49)$$

and likewise

$$\begin{aligned} &I(m_A, h_{BA}^K, y_A^{N-1}; y_B(N) | \mathbf{z}^N, \mathbf{g}^K, m_B, h_{AB}^K, y_B^{N-1}) \\ &\leq I(x_A(N); y_B(N) | z_{AE}(N), h_{AB}(N), g_{AE}(N)). \end{aligned} \quad (50)$$

Finally using the fact that $x_A(N)$ and $x_B(N)$ are functions of (m_A, y_{BA}^{N-1}) and (m_B, y_{AB}^{N-1}) respectively and the fact that $y_A(N)$ is independent of all other random variables given $(x_A(N), h_{AB}(N))$ and similarly $y_B(N)$ is independent of all other random variables given $(x_B(N), h_{BA}(N))$ we can show that

$$\begin{aligned} &I(y_A(N); y_B(N) | \mathbf{z}^N, \mathbf{g}^K, m_B, h_{AB}^K, y_B^{N-1}, m_A, h_{BA}^K, y_A^{N-1}) \\ &= 0. \end{aligned} \quad (51)$$

Thus substituting (48), (49) and (50) into (41) we have that

$$\begin{aligned} NR &\leq I(m_A, h_{BA}^K, y_A^{N-1}; m_B, h_{AB}^K, y_B^{N-1} | \mathbf{z}^{N-1}, \mathbf{g}^K) \\ &\quad + I(y_A(N); x_B(N) | z_{BE}(N), g_{BE}(N), h_{BA}(N)) \\ &\quad + I(x_A(N); y_B(N) | z_{AE}(N), h_{AB}(N), g_{AE}(N)) \end{aligned} \quad (52)$$

Recursively applying the same steps we have that

$$\begin{aligned} NR &\leq I(m_A, h_{BA}^K; h_{AB}^K, m_B | \mathbf{g}^K) + \\ &\quad \sum_{i=1}^N I(x_B(i); y_A(i) | z_{BE}(i), g_{BE}(i), h_{BA}(i)) + \\ &\quad \sum_{i=1}^N I(x_A(i); y_B(i) | z_{AE}(i), g_{AE}(i), h_{AB}(i)) \quad (53) \\ &= KI(h_{BA}; h_{AB}) + \\ &\quad \sum_{i=1}^N I(x_B(i); y_A(i) | z_{BE}(i), g_{BE}(i), h_{BA}(i)) + \\ &\quad \sum_{i=1}^N I(x_A(i); y_B(i) | z_{AE}(i), g_{AE}(i), h_{AB}(i)) \end{aligned} \quad (54)$$

where in (54) we use the fact that (m_A, m_B) are mutually independent and independent of the channel gains and furthermore (h_{AB}^K, h_{BA}^K) are independent of \mathbf{g}^K . Finally to establish the upper bound (3) suppose that we assign a power $P_i(h_{AB})$ when the channel gain at time i equals h_{AB} . Using the fact that a Gaussian input distribution maximizes the conditional mutual information terms in (54) (see e.g., [41]) we have:

$$\begin{aligned} &I(x_A(i); y_B(i) | z_{AE}(i), g_{AE}(i), h_{AB}(i)) \\ &\leq E \left[\log \left(1 + \frac{P_i(h_{AB}) |h_{AB}|^2}{1 + P_i(h_{AB}) |g_{AE}|^2} \right) \right]. \end{aligned} \quad (55)$$

Thus we have that

$$\begin{aligned} &\sum_{i=1}^N I(x_A(i); y_B(i) | z_{AE}(i), g_{AE}(i), h_{AB}(i)) \\ &\leq \sum_{i=1}^N E \left[\log \left(1 + \frac{P_i(h_{AB}) |h_{AB}|^2}{1 + P_i(h_{AB}) |g_{AE}|^2} \right) \right] \end{aligned} \quad (56)$$

$$= E \left[\sum_{i=1}^N \log \left(1 + \frac{P_i(h_{AB}) |h_{AB}|^2}{1 + P_i(h_{AB}) |g_{AE}|^2} \right) \right] \quad (57)$$

$$I(m_A, h_{BA}^K, y_A^{N-1}; m_B, h_{AB}^K, y_B^{N-1} | \mathbf{z}^N, \mathbf{g}^K) \quad (42)$$

$$\leq I(m_A, h_{BA}^K, y_A^{N-1}, z_{AE}(N); m_B, h_{AB}^K, y_B^{N-1}, z_{BE}(N) | \mathbf{z}^{N-1}, \mathbf{g}^K) \quad (43)$$

$$= I(m_A, h_{BA}^K, y_A^{N-1}; m_B, h_{AB}^K, y_B^{N-1}, z_{BE}(N) | \mathbf{z}^{N-1}, \mathbf{g}^K) \\ + I(z_{AE}(N); m_B, h_{AB}^K, y_B^{N-1}, z_{BE}(N) | \mathbf{z}^{N-1}, \mathbf{g}^K, m_A, h_{BA}^K, y_A^{N-1}) \quad (44)$$

$$= I(m_A, h_{BA}^K, y_A^{N-1}; m_B, h_{AB}^K, y_B^{N-1}, z_{BE}(N) | \mathbf{z}^{N-1}, \mathbf{g}^K) \quad (45)$$

$$= I(m_A, h_{BA}^K, y_A^{N-1}; m_B, h_{AB}^K, y_B^{N-1} | \mathbf{z}^{N-1}, \mathbf{g}^K) + I(m_A, h_{BA}^K, y_A^{N-1}; z_{BE}(N) | \mathbf{z}^{N-1}, \mathbf{g}^K, m_B, h_{AB}^K, y_B^{N-1}) \quad (46)$$

$$= I(m_A, h_{BA}^K, y_A^{N-1}; m_B, h_{AB}^K, y_B^{N-1} | \mathbf{z}^{N-1}, \mathbf{g}^K) \quad (47)$$

$$\leq NE \left[\log \left(1 + \frac{\frac{1}{N} \sum_{i=1}^N P_i(h_{AB}) |h_{AB}|^2}{1 + \frac{1}{N} \sum_{i=1}^N P_i(h_{AB}) |g_{AE}|^2} \right) \right] \quad (58)$$

$$= NE \left[\log \left(1 + \frac{P(h_{AB}) |h_{AB}|^2}{1 + P(h_{AB}) |g_{AE}|^2} \right) \right], \quad (59)$$

$$= NI(x_A; y_B | z_{AE}, g_{AE}, h_{AB}) \quad (60)$$

where $P(h_{AB}) \triangleq \frac{1}{N} \sum_{i=1}^N P_i(h_{AB})$ is the average power allocated when the fading state equals h_{AB} and (58) uses the fact that the function $f(x) = \log \left(1 + \frac{ax}{1+bx} \right)$ is a concave function in x and hence Jensen's inequality applies. Also note that

$$E[P(h_{AB})] = E \left[\frac{1}{N} \sum_{i=1}^N P_i(h_{AB}) \right] \quad (61)$$

$$= \frac{1}{N} \sum_{i=1}^N E[P_i(h_{AB})] \quad (62)$$

$$\leq \frac{1}{N} \sum_{i=1}^N P_i \leq P. \quad (63)$$

In a similar fashion we can show that

$$\sum_{i=1}^N I(x_B(i); y_A(i) | z_{BE}(i), g_{BE}(i), h_{BA}(i)) \\ \leq NE \left[\log \left(1 + \frac{P(h_{BA}) |h_{BA}|^2}{1 + P(h_{BA}) |g_{BE}|^2} \right) \right]. \quad (64)$$

$$= NI(x_B; y_A | z_{BE}, g_{BE}, h_{BA}) \quad (65)$$

The upper bound (3) follows by substituting in (60) and (65) into (54). This completes the proof of Theorem 1.

IV. PROOF OF THEOREM 2

We sketch the coding scheme associated with Theorem 2, where we assume the availability of a public discussion channel. In our proof we assume that the channel input and output symbols as well as the fading gains are discrete valued. We do not address the discretization of these random variables in this section; it will be addressed in the proof of Theorem 3, when we do not assume the availability of a discussion channel.

A. Generation of Correlated Source Sequences

In each coherence block we reserve the first symbol for transmission of a pilot symbol

$$x_A(iT + 1) = x_B(iT + 1) = \sqrt{P_1}, \\ i = 0, \dots, \frac{N}{T} - 1. \quad (66)$$

and the remainder of the symbols for transmission of i.i.d. random variables i.e.,

$$x_A(t) \sim p_{x_A}(\cdot), x_B(t) \sim p_{x_B}(\cdot), \forall t \in [1, N], t \neq iT + 1. \quad (67)$$

The legitimate receivers B and A use the corresponding output symbols $y_B(iT + 1)$ and $y_A(iT + 1)$ for estimating the underlying channel gains $\hat{h}_{AB}(i + 1)$ and $\hat{h}_{BA}(i + 1)$ in (5) and (6) respectively.

We use the bold-font notation $\bar{\mathbf{x}}_A(t)$ to denote the sequence of $T - 1$ i.i.d. symbols transmitted in coherence block t . and let $\bar{\mathbf{y}}_B(t)$ denote the corresponding output symbol vector in block t . The source sequences at the terminals at the end of K coherence blocks are indicated in Table I.

B. Information Reconciliation

Terminals A and B exchange public messages over the discussion channel to agree on identical sequence pair $(\hat{h}_{AB}^K, \hat{h}_{BA}^K, \bar{\mathbf{y}}_{AB}^K, \bar{\mathbf{y}}_{BA}^K)$. The public messages transmitted are as follows (i) Terminal A bins the sequences $\{\hat{h}_{BA}^K\}$ into $2^{K(H(\hat{h}_{BA}|\hat{h}_{AB})+\epsilon)}$ bins and transmits the associated bin index ϕ_A over the discussion channel. (ii) Terminal B bins the sequences $\{\hat{h}_{AB}^K\}$ into $2^{K(H(\hat{h}_{AB}|\hat{h}_{BA})+\epsilon)}$ bins and transmits the associated bin index ϕ_B over the discussion channel. (iii) Terminal A bins the sequences $\{\bar{\mathbf{y}}_A^K\}$ into $2^{K(H(\bar{\mathbf{y}}_A|\bar{\mathbf{x}}_B, \hat{h}_{AB}, \hat{h}_{BA})+\epsilon)}$ and transmits the associated bin index ψ_A over the discussion channel. (iv) Terminal B bins the sequence $\{\bar{\mathbf{y}}_B^K\}$ into $2^{K(H(\bar{\mathbf{y}}_B|\bar{\mathbf{x}}_A, \hat{h}_{AB}, \hat{h}_{BA})+\epsilon)}$ and transmits the associated bin index ψ_B over the discussion channel.

Using standard arguments (see e.g., [42, Chap. 10]) Terminal A can reconstruct the sequence pair $(\hat{h}_{AB}^K, \bar{\mathbf{y}}_B^K)$ (with high probability) given the messages (ϕ_B, ψ_B) and its side information $(\hat{h}_{BA}^K, \bar{\mathbf{x}}_A^K)$. Terminal B can reconstruct the sequence pair $(\hat{h}_{BA}^K, \bar{\mathbf{y}}_A^K)$ (with high probability) given the messages (ϕ_A, ψ_A) and its side information sequence $(\hat{h}_{AB}^K, \bar{\mathbf{x}}_B^K)$. Thus at the end of this phase both terminals have access to the common sequence pair $(\bar{\mathbf{y}}_A^K, \bar{\mathbf{y}}_B^K, \hat{h}_{AB}^K, \hat{h}_{BA}^K)$. The eavesdropper has access to $(\bar{\mathbf{z}}^K, \mathbf{g}^K, \phi_A, \phi_B, \psi_A, \psi_B)$.

C. Equivocation Analysis

We lower bound the equivocation at the eavesdropper as follows:

$$\begin{aligned} & H(\bar{\mathbf{y}}_A^K, \bar{\mathbf{y}}_B^K, \hat{h}_{AB}^K, \hat{h}_{BA}^K | \bar{\mathbf{z}}^K, \mathbf{g}^K, \phi_A, \phi_B, \psi_A, \psi_B) \\ &= H(\bar{\mathbf{y}}_A^K, \bar{\mathbf{y}}_B^K, \hat{h}_{AB}^K, \hat{h}_{BA}^K | \bar{\mathbf{z}}^K, \mathbf{g}^K) - H(\phi_A) - H(\phi_B) \\ &\quad - H(\psi_A) - H(\psi_B) \\ &= H(\hat{h}_{AB}^K, \hat{h}_{BA}^K) + H(\bar{\mathbf{y}}_A^K, \bar{\mathbf{y}}_B^K | \bar{\mathbf{z}}^K, \mathbf{g}^K, \hat{h}_{AB}^K, \hat{h}_{BA}^K) \\ &\quad - H(\phi_A) - H(\phi_B) - H(\psi_A) - H(\psi_B) \end{aligned} \quad (68)$$

$$\begin{aligned} & \geq H(\hat{h}_{AB}^K, \hat{h}_{BA}^K) + H(\bar{\mathbf{y}}_A^K, \bar{\mathbf{y}}_B^K | \bar{\mathbf{z}}^K, \mathbf{g}^K, \hat{h}_{AB}^K, \hat{h}_{BA}^K) \\ &\quad - H(\phi_A) - H(\phi_B) - H(\psi_A) - H(\psi_B) \end{aligned} \quad (69)$$

$$\begin{aligned} &= H(\hat{h}_{AB}^K, \hat{h}_{BA}^K) + H(\bar{\mathbf{y}}_A^K | \bar{\mathbf{z}}_B^K, \mathbf{g}_{BE}^K, \hat{h}_{BA}^K) \\ &\quad + H(\bar{\mathbf{y}}_B^K | \bar{\mathbf{z}}_A^K, \mathbf{g}_{AE}^K, \hat{h}_{AB}^K) \\ &\quad - H(\phi_A) - H(\phi_B) - H(\psi_A) - H(\psi_B) \end{aligned} \quad (70)$$

$$\begin{aligned} &= KH(\hat{h}_{AB}, \hat{h}_{BA}) + KH(\bar{\mathbf{y}}_A | \bar{\mathbf{z}}_B, \mathbf{g}_{BE}, h_{BA}) \\ &\quad + KH(\bar{\mathbf{y}}_B | \bar{\mathbf{z}}_A, \mathbf{g}_{AE}, h_{AB}) \\ &\quad - H(\phi_A) - H(\phi_B) - H(\psi_A) - H(\psi_B) \end{aligned} \quad (71)$$

where we use the chain rule of entropy and the fact that $(\hat{h}_{AB}^K, \hat{h}_{BA}^K)$ is independent of $(\bar{\mathbf{z}}^K, \mathbf{g}^K)$ in (68); in (69) we use the fact that conditioning reduces entropy as well as \hat{h}_{AB}^K and \hat{h}_{BA}^K are independent of the remaining variables gives \hat{h}_{AB}^K and \hat{h}_{BA}^K respectively; in (70) we use the fact that $\bar{\mathbf{x}}_A^K$ and $\bar{\mathbf{x}}_B^K$ are sampled independently and hence the following Markov conditions hold:

$$\bar{\mathbf{y}}_A^K \rightarrow (\bar{\mathbf{z}}_B^K, \mathbf{g}_{BE}^K, h_{BA}^K) \rightarrow (\bar{\mathbf{y}}_B^K, \mathbf{g}_{AE}^K, \hat{h}_{AB}^K) \quad (72)$$

$$\bar{\mathbf{y}}_B^K \rightarrow (\bar{\mathbf{z}}_A^K, \mathbf{g}_{AE}^K, \hat{h}_{AB}^K) \rightarrow (\bar{\mathbf{y}}_A^K, \mathbf{g}_{BE}^K, \hat{h}_{BA}^K); \quad (73)$$

Eq. (71) follows from the fact that the sequence pair (h_{AB}^K, h_{BA}^K) is sampled i.i.d. and furthermore $\bar{\mathbf{x}}_A^K$ and $\bar{\mathbf{x}}_B^K$ are also sampled i.i.d. Furthermore,

$$\begin{aligned} & KH(h_{AB}, h_{BA}) - H(\phi_A) - H(\phi_B) \\ & \geq KH(\hat{h}_{AB}, \hat{h}_{BA}) - H(\hat{h}_{BA} | \hat{h}_{AB}) - H(\hat{h}_{AB} | \hat{h}_{BA}) - 4K\varepsilon \end{aligned} \quad (74)$$

$$= KI(\hat{h}_{AB}, \hat{h}_{BA}) - 4K\varepsilon. \quad (75)$$

Using the fact that $\bar{\mathbf{x}}_A$ is sampled i.i.d. in (77) and letting $\varepsilon' = \frac{\varepsilon}{T-1}$ we have

$$\begin{aligned} & KH(\bar{\mathbf{y}}_A | \bar{\mathbf{z}}_B, \mathbf{g}_{BE}, h_{BA}) - H(\psi_A) \\ & \geq KH(\bar{\mathbf{y}}_A | \bar{\mathbf{z}}_B, \mathbf{g}_{BE}, h_{BA}) - KH(\bar{\mathbf{y}}_A | \bar{\mathbf{x}}_B, \hat{h}_{AB}, \hat{h}_{BA}) - 2K\varepsilon \end{aligned} \quad (76)$$

$$= K(T-1) \left\{ H(y_A | z_B, \mathbf{g}_{BE}, h_{BA}) - H(y_A | x_B, \hat{h}_{AB}, \hat{h}_{BA}) - 2\varepsilon' \right\} \quad (77)$$

$$= K(T-1) \left\{ I(y_A; x_B, \hat{h}_{AB}, \hat{h}_{BA}) - I(y_A; z_B, \mathbf{g}_{BE}, h_{BA}) - 2\varepsilon' \right\}. \quad (78)$$

In a similar fashion we can show that

$$\begin{aligned} & KH(\bar{\mathbf{y}}_B | \bar{\mathbf{z}}_A, \mathbf{g}_{AE}, h_{AB}) - H(\psi_B) \\ & \geq K(T-1) \left\{ I(y_B; x_A, \hat{h}_{AB}, \hat{h}_{BA}) - I(y_B; z_A, \mathbf{g}_{AE}, h_{AB}) - 2\varepsilon' \right\} \end{aligned} \quad (79)$$

Combining (75), (78) and (79) we obtain that

$$\begin{aligned} & H(\bar{\mathbf{y}}_A^K, \bar{\mathbf{y}}_B^K, \hat{h}_{AB}^K, \hat{h}_{BA}^K | \bar{\mathbf{z}}^K, \mathbf{g}^K, \phi_A, \phi_B, \psi_A, \psi_B) \\ & \geq KI(\hat{h}_{AB}, \hat{h}_{BA}) - 4K\varepsilon - 4K\varepsilon' \\ & \quad + K(T-1) \left\{ I(y_A; x_B, \hat{h}_{AB}, \hat{h}_{BA}) - I(y_A; z_B, \mathbf{g}_{BE}, h_{BA}) - 2\varepsilon' \right\} \\ & \quad + K(T-1) \left\{ I(y_B; x_A, \hat{h}_{AB}, \hat{h}_{BA}) - I(y_B; z_A, \mathbf{g}_{AE}, h_{AB}) - 2\varepsilon' \right\} \end{aligned} \quad (80)$$

In the final step, the equivocation lower bound in (80) can be used to generate a secret-key. The associated construction is discussed in section V-G when we consider the case without a public discussion channel. We omit the details as they are completely analogous.

D. Proof of Prop. 1

We evaluate the rate expression (8) in Theorem 2 by selecting $x_A \sim \mathcal{CN}(0, P_2)$ and $x_B \sim \mathcal{CN}(0, P_2)$. Note that the MMSE estimates of h_{AB} and h_{BA} can be expressed as

$$\hat{h}_{AB} = \alpha h_{AB} + e_{AB} \quad (81)$$

$$\hat{h}_{BA} = \alpha h_{BA} + e_{BA} \quad (82)$$

where $\alpha = \frac{P_1}{P_1+1}$ is the linear MMSE coefficient and $e_{AB}, e_{BA} \sim \mathcal{CN}(0, \alpha(1-\alpha))$ are mutually independent and independent of (h_{AB}, h_{BA}) .

Thus \hat{h}_{AB} and \hat{h}_{BA} are jointly Gaussian random variables with $E[|\hat{h}_{AB}|^2] = E[|\hat{h}_{BA}|^2] = \alpha$ and $E[\hat{h}_{AB}\hat{h}_{BA}^*] = \alpha^2 E[h_{AB}h_{BA}^*]$. Hence one can show that

$$I(\hat{h}_{AB}, \hat{h}_{BA}) = -\log(1 - \alpha^2 \rho^2). \quad (83)$$

To compute the remaining terms in (8) note that

$$\begin{aligned} & I(y_A; x_B, \hat{h}_{AB}, \hat{h}_{BA}) - I(y_A; z_B, \mathbf{g}_{BE}, h_{BA}) \\ & \geq h(y_A | z_B, \mathbf{g}_{BE}, h_{BA}) - h(y_A | x_B, \hat{h}_{AB}, \hat{h}_{BA}) \end{aligned} \quad (84)$$

$$\geq h(y_A | z_B, \mathbf{g}_{BE}, h_{BA}) - h(y_A | x_B, \hat{h}_{BA}) \quad (85)$$

The since $x_B \sim \mathcal{CN}(0, P_2)$, the first-term can be evaluated as:

$$h(y_A | z_B, \mathbf{g}_{BE}, h_{BA}) = E \left[\log 2\pi e \left(1 + \frac{P_2 |h_{BA}|^2}{1 + P_2 |\mathbf{g}_{BE}|^2} \right) \right]. \quad (86)$$

To evaluate the second term we introduce $\tilde{h}_{BA} \triangleq h_{BA} - \hat{h}_{BA}$. Note that since \hat{h}_{BA} is the MMSE estimate of h_{BA} , we have that $\tilde{h}_{BA} \sim \mathcal{CN}(0, \frac{1}{1+P_1})$ and hence

$$h(y_A | x_B, \hat{h}_{BA}) \leq h(y_A - \hat{h}_{BA} x_B) \quad (87)$$

$$= h(\tilde{h}_{BA} x_B + z_B) \quad (88)$$

$$\leq \log 2\pi e \left(1 + \frac{P_2}{1 + P_1} \right) \quad (89)$$

where we use the fact that conditioning reduces the differential entropy in (88) and that Gaussian distribution maximizes entropy among all distributions with a fixed variance in (89).

From (85), (86) and (89) we have that

$$R_{P,BA}^- = I(y_A; x_B, \hat{h}_{AB}, \hat{h}_{BA}) - I(y_A; z_B, \mathbf{g}_{BE}, h_{BA}) \quad (90)$$

$$= E \left[\log \left(1 + \frac{P_2 |h_{BA}|^2}{1 + P_2 |g_{BE}|^2} \right) \right] - \log \left(1 + \frac{P_2}{1 + P_1} \right) \quad (91)$$

which establishes (13). The expression (12) for $R_{P,AB}^-$ can be established in a similar manner.

V. PROOF OF THEOREM 3

In absence of the discussion channel, we need to transmit the public messages during the error-reconciliation phase using the same wireless channel. We again use K coherence blocks to generate source and channel sequences as in Table I using the training and communication phases as in (66) and (67). Thereafter we use $\varepsilon_1 \cdot K$ coherence blocks for generating the secret-key from the channel sequences and another $\varepsilon_2 \cdot K$ coherence blocks for generating the secret-key from the source sequences. Due to this overhead, the total rate achieved is scaled by a factor of $\frac{1}{1+\varepsilon_1+\varepsilon_2}$ as in (26).

In the secret-key generation phase we suitably quantize each of the channel-state and source sequences to satisfy the rate constraint for public messages. We describe the key steps of the coding scheme below.

A. Quantization of Continuous Valued Random Variables

While our lower bound is stated for continuous valued random variables, in the analysis of our coding scheme, we follow the approach in [42, pp. 50, sec. 3.4.1] and assume that associated random variables are discrete valued. In particular let $x_B \sim p_{x_B}(\cdot)$ be any continuous and bounded density function. We consider an associated quantized version of x_B , $[x_B]_j \in \{-j\Delta, -(j-1)\Delta, \dots, (j-1)\Delta, j\Delta\}$, with $\Delta = \frac{1}{\sqrt{J}}$, obtained by mapping x_B to the closest quantization point such that $|[x_B]_j| \leq |x_B|$ holds. Likewise for $y_{A,j} = h_{BA}[x_B]_j + n_A$, let $[y_{A,j}]_k$ be defined in a similar manner. The random variables $[x_A]_j$ and $[y_{B,j}]_k$ as well as the variables $[u_{BA}]_k$, $[u_{AB}]_k$, $[v_A]_k$ and $[v_B]_k$ associated with the quantization codebooks are defined analogously. As we make the quantization finer and finer, the rate using these discrete random variables will approach the proposed lower bound with continuous valued random variables [42, pp. 65, sec. 3.8]. In what follows, we will treat these random variables as discrete valued and use the notion of robust-typicality [42, pp. 25-31, sec. 2.4].

B. Codebook Construction

Suitable quantization codebooks for the source and channel sequences are necessary in order to satisfy the rate-constraint associated with the wireless channel. Table II illustrates the different quantization codebooks used in our coding scheme, which are further described below.

- **(Channel Quantization, Node A)** \mathcal{C}_A^u : We sample a total of $M_A^u = 2^{K(I(u_{BA}; \hat{h}_{BA}) + \varepsilon)}$ codewords $\{u_{BA}^K\}$ i.i.d. each of length K , according to a distribution $p_{u_{BA}}(\cdot)$. These codewords are divided into a total of $T_A^u = 2^{K(I(u_{BA}; \hat{h}_{BA} | \hat{h}_{AB}) + 2\varepsilon)}$ bins such that there are $N_A^u = 2^{K(I(u_{BA}; \hat{h}_{AB}) - \varepsilon)}$ codewords per bin.
- **(Channel Quantization, Node B)** \mathcal{C}_B^u : We sample a total of $M_B^u = 2^{K(I(u_{AB}; \hat{h}_{AB}) + \varepsilon)}$ codewords $\{u_{AB}^K\}$ i.i.d.

according to a distribution $p_{u_{AB}}(\cdot)$. These codewords are divided into a total of $T_B^u = 2^{K(I(u_{AB}; \hat{h}_{AB} | \hat{h}_{BA}) + 2\varepsilon)}$ bins such that there are $N_B^u = 2^{K(I(u_{AB}; \hat{h}_{BA}) - \varepsilon)}$ codewords per bin.

- **(Source Quantization, Node A)** \mathcal{C}_A^v : We sample a total of $M_A^v = 2^{K(I(\bar{v}_A; \bar{y}_A) + \varepsilon)}$ codewords $\{\bar{v}_A^K\}$ i.i.d. according to the distribution $p_{\bar{v}_A}(\cdot)$. These codewords are partitioned into a total of $T_A^v = 2^{K(I(\bar{v}_A; \bar{y}_A | \bar{x}_B, u) + 2\varepsilon)}$ bins such that there are $N_B^v = 2^{K(I(\bar{v}_A; \bar{x}_B, u) - \varepsilon)}$ codewords per bin.
- **(Source Quantization, Node B)** \mathcal{C}_B^v : We sample a total of $M_B^v = 2^{K(I(\bar{v}_B; \bar{y}_B) + \varepsilon)}$ codewords $\{\bar{v}_B^K\}$ i.i.d. according to the distribution $p_{\bar{v}_B}(\cdot)$. These codewords are partitioned into a total of $T_B^v = 2^{K(I(\bar{v}_B; \bar{y}_B | \bar{x}_A, u) + 2\varepsilon)}$ bins such that there are $N_B^v = 2^{K(I(\bar{v}_B; \bar{x}_A, u) - \varepsilon)}$ codewords per bin.

C. Encoding

- Terminal A finds a codeword $u_{BA}^K \in \mathcal{C}_A^u$ that is jointly typical with \hat{h}_{BA}^K . It finds the bin index ϕ_A of u_{BA}^K and transmits it as a public message over the channel.
- Terminal B finds a codeword $u_{AB}^K \in \mathcal{C}_B^u$ that is jointly typical with \hat{h}_{AB}^K . It finds the bin index ϕ_B of u_{AB}^K and transmits it as a public message over the channel.
- Terminal A finds a codeword $\bar{v}_A^K \in \mathcal{C}_A^v$ that is jointly typical with \bar{y}_A^K . It finds the bin index ψ_A of \bar{v}_A^K and transmits it as a public message over the channel.
- Terminal B finds a codeword $\bar{v}_B^K \in \mathcal{C}_B^v$ that is jointly typical with \bar{y}_B^K . It finds the bin index ψ_B of \bar{v}_B^K and transmits it as a public message over the channel.

We let \mathcal{J}_1 denote the error event that either terminal A or terminal B fails to find a codeword sequence typical with the source sequence and let \mathcal{J}_2 denote the error event associated with the transmission of the public message.

D. Decoding

Terminal A, upon receiving ϕ_B , searches for a codeword u_{AB}^K in the bin-index $\phi_B \in \mathcal{C}_B^u$ that is jointly typical with \hat{h}_{BA}^K . It declares an error if none or more than one sequence are jointly typical. Terminal A, upon receiving ψ_B , searches for a codeword \bar{v}_B^K in the bin-index $\psi_B \in \mathcal{C}_B^v$ that is jointly typical with (\bar{y}_A^K, u^K) . It declares an error if none or more than one sequence appears to be typical. We define $\mathcal{E}_1 = \Pr(\hat{u}_{AB}^K \neq u_{AB}^K \cup \hat{\bar{v}}_B^K \neq \bar{v}_B^K)$.

Terminal B, upon receiving ϕ_A , searches for a codeword u_{BA}^K in the bin-index $\phi_A \in \mathcal{C}_A^u$ that is jointly typical with \hat{h}_{AB}^K . It declares an error if none or more than one sequences are jointly typical. Terminal B, upon receiving ψ_A , searches for a codeword \bar{v}_A^K in the bin-index $\psi_A \in \mathcal{C}_A^v$ that is jointly typical with (\bar{y}_B^K, u^K) . It declares an error if none or more than one sequence appears to be typical. We define $\mathcal{E}_2 = \Pr(\hat{u}_{BA}^K \neq u_{BA}^K \cup \hat{\bar{v}}_A^K \neq \bar{v}_A^K)$.

E. Error Analysis (Sketch)

Let $\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{J}_1 \cup \mathcal{J}_2$ denote the union of all error events. It suffices to show that both \mathcal{E}_i and \mathcal{J}_i have vanishing probabilities for $i \in \{1, 2\}$. Since the total number of codeword sequences in \mathcal{C}_A^u equals $2^{K(I(u_{BA}; \hat{h}_{BA}) + \varepsilon)}$, it follows

TABLE II
QUANTIZATION CODEBOOKS FOR SOURCE AND CHANNEL SEQUENCES

Codebook	Total Codewords	Total Bins	Codewords Per Bin
Channel Quantization (Node A): \mathcal{C}_A^u	$2^{K(I(u_{BA}; \hat{h}_{BA}) + \varepsilon)}$	$2^{K(I(u_{BA}; \hat{h}_{BA} \hat{h}_{AB}) + 2\varepsilon)}$	$2^{K(I(u_{BA}; \hat{h}_{AB}) - \varepsilon)}$
Channel Quantization (Node B): \mathcal{C}_B^u	$2^{K(I(u_{AB}; \hat{h}_{AB}) + \varepsilon)}$	$2^{K(I(u_{AB}; \hat{h}_{AB} \hat{h}_{BA}) + 2\varepsilon)}$	$2^{K(I(u_{AB}; \hat{h}_{BA}) - \varepsilon)}$
Source Quantization (Node A): \mathcal{C}_A^v	$2^{K(I(\mathbf{v}_A; \mathbf{y}_A) + \varepsilon)}$	$2^{K(I(\mathbf{v}_A; \mathbf{y}_A \mathbf{x}_B, \mathbf{u}) + 2\varepsilon)}$	$2^{K(I(\mathbf{v}_A; \mathbf{x}_B, \mathbf{u}) - \varepsilon)}$
Source Quantization (Node B): \mathcal{C}_B^v	$2^{K(I(\mathbf{v}_B; \mathbf{y}_B) + \varepsilon)}$	$2^{K(I(\mathbf{v}_B; \mathbf{y}_B \mathbf{x}_A, \mathbf{u}) + 2\varepsilon)}$	$2^{K(I(\mathbf{v}_B; \mathbf{x}_A, \mathbf{u}) - \varepsilon)}$

from the Covering Lemma [42, pp. 62, Lemma 3.3] that the probability that no jointly typical codeword exists goes to zero as $K \rightarrow \infty$. By a similar argument we have that $\Pr(\mathcal{J}_1) \rightarrow 0$. Since $H(\phi_A) \leq K(I(u_{BA}; \hat{h}_{BA} | \hat{h}_{AB}) + 2\varepsilon)$ and since the rate constraint (18) is imposed, terminal B decodes ϕ_A with high probability. In a similar fashion it can be argued that $\Pr(\mathcal{J}_2) \rightarrow 0$ as $K \rightarrow \infty$. Since the total number of codewords in each bin of \mathcal{C}_B^u is $2^{K(I(u_{AB}; \hat{h}_{AB}) - \varepsilon)}$ it follows from the Packing Lemma [42, pp. 46, Lemma 3.1] that terminal A will decode $\{\hat{u}_{AB}^K = u_{AB}^K\}$ with high probability. By analogous arguments it can be verified that $\Pr(\mathcal{E}_1) \rightarrow 0$ and $\Pr(\mathcal{E}_2) \rightarrow 0$ as $K \rightarrow \infty$.

F. Equivocation Analysis

Let us define $\mathbf{z}^K = (\mathbf{z}_A^K, \mathbf{z}_B^K)$ and $\mathbf{g}^K = (g_{AE}^K, g_{BE}^K)$. We first consider the conditional entropy term¹

$$\begin{aligned} H(u_{BA}^K, u_{AB}^K, \mathbf{v}_A^K, \mathbf{v}_B^K | \phi_A, \phi_B, \psi_A, \psi_B, \mathbf{z}^K, \mathbf{g}^K) &\geq \\ &\geq H(u_{BA}^K, u_{AB}^K, \mathbf{v}_A^K, \mathbf{v}_B^K | \mathbf{z}^K, \mathbf{g}^K) - H(\phi_A) \\ &\quad - H(\phi_B) - H(\psi_A) - H(\psi_B) \end{aligned} \quad (92)$$

$$\begin{aligned} &= H(u_{BA}^K, u_{AB}^K | \mathbf{z}^K, \mathbf{g}^K) \\ &\quad + H(\mathbf{v}_A^K, \mathbf{v}_B^K | u_{BA}^K, u_{AB}^K, \mathbf{z}^K, \mathbf{g}^K) \\ &\quad - H(\phi_A) - H(\phi_B) - H(\psi_A) - H(\psi_B) \end{aligned} \quad (93)$$

$$\begin{aligned} &= H(u_{BA}^K, u_{AB}^K) + H(\mathbf{v}_A^K, \mathbf{v}_B^K | u_{BA}^K, u_{AB}^K, \mathbf{z}^K, \mathbf{g}^K) \\ &\quad - H(\phi_A) - H(\phi_B) - H(\psi_A) - H(\psi_B) \end{aligned} \quad (94)$$

where (94) follows from the fact that (u_{BA}^K, u_{AB}^K) are independent of $(\mathbf{x}_A^K, \mathbf{x}_B^K)$ and hence $(\mathbf{z}^K, \mathbf{g}^K)$.

From the construction recall that ϕ_A, ϕ_B, ψ_A and ψ_B denote the bin indices in $\mathcal{C}_A^u, \mathcal{C}_B^u, \mathcal{C}_A^v$ and \mathcal{C}_B^v respectively. Therefore

$$H(\phi_A) \leq I(u_{BA}; \hat{h}_{BA} | \hat{h}_{AB}) + 2\varepsilon, \quad (95)$$

$$H(\phi_B) \leq I(u_{AB}; \hat{h}_{AB} | \hat{h}_{BA}) + 2\varepsilon, \quad (96)$$

$$H(\psi_A) \leq I(\mathbf{v}_A; \mathbf{y}_A | \mathbf{x}_B, \mathbf{u}) + 2\varepsilon, \quad (97)$$

$$H(\psi_B) \leq I(\mathbf{v}_B; \mathbf{y}_B | \mathbf{x}_A, \mathbf{u}) + 2\varepsilon. \quad (98)$$

Thus we need to lower bound the joint-entropy terms in (94). We use the following Lemma.

Lemma 1: Consider a triplet of random variables (u, x, y) that satisfy $u \rightarrow x \rightarrow y$. Suppose that the sequence x^n is sampled i.i.d. $p_x(\cdot)$. Suppose that we generate a set \mathcal{A} consisting of $M = 2^{nR}$ sequences $\{u^n(i)\}_{1 \leq i \leq M}$ each sampled i.i.d. from a distribution $p_u(\cdot)$. Given x^n we select an index L such that $(x^n, u^n(L)) \in \mathcal{T}_\varepsilon^n(x, u)$. If no such index exists we

select L uniformly at random. If y^n is sampled i.i.d. from the conditional distribution $p_{y|x}(\cdot | \cdot)$, then

$$H(y^n | u^n(L)) \geq n \{H(y|u) + I(x; u) - R - \gamma_n(\varepsilon)\} \quad (99)$$

for any $R > I(x; u)$ and for some $\gamma_n(\varepsilon)$ that goes to zero as $\varepsilon \rightarrow 0$ and $n \rightarrow \infty$.

Proof: See Appendix A ■

We first lower bound the term $H(u_{BA}^K, u_{AB}^K)$. Notice that $u_{BA}^K \rightarrow \hat{h}_{BA}^K \rightarrow u_{AB}^K$ holds. Since u_{BA}^K and u_{AB}^K are distributed, nearly uniformly on the codebooks \mathcal{C}_A^u and \mathcal{C}_B^u respectively (see e.g., [43, pp. 660, Lemma 1]) we have that

$$H(u_{BA}^K) \geq K(I(u_{BA}; \hat{h}_{BA}) - \gamma_K(\varepsilon)) \quad (100)$$

$$H(u_{AB}^K) \geq K(I(u_{AB}; \hat{h}_{AB}) - \gamma_K(\varepsilon)) \quad (101)$$

Substituting $x = \hat{h}_{AB}$, $y = \hat{h}_{BA}$ and $u = u_{BA}$ and $R = I(u_{BA}; \hat{h}_{AB}) + 2\varepsilon$ in Lemma 1 we have that

$$H(\hat{h}_{BA}^K | u_{BA}^K) \geq K \left\{ H(\hat{h}_{BA} | u_{BA}) - \gamma_K(\varepsilon) \right\}. \quad (102)$$

We define the indicator function $\mathbb{I}_\varepsilon(\hat{h}_{BA}^K, u_{AB}^K, u_{BA}^K)$ to equal 1 if $(\hat{h}_{BA}^K, u_{AB}^K, u_{BA}^K) \in \mathcal{T}_\varepsilon^K$ and zero otherwise. Using the Markov Lemma [42, sec 12.1.1] we have that $\Pr(\mathbb{I}(\hat{h}_{BA}^K, u_{AB}^K, u_{BA}^K) = 1) \rightarrow 1$ as $K \rightarrow \infty$ for every $\varepsilon > 0$. Hence

$$H(\hat{h}_{BA}^K | u_{BA}^K, u_{AB}^K) \leq H(\hat{h}_{BA}^K | u_{BA}^K, u_{AB}^K, \mathbb{I}_\varepsilon) + 1 \quad (103)$$

$$\leq H(\hat{h}_{BA}^K | u_{BA}^K, u_{AB}^K, \mathbb{I}_\varepsilon = 1) \Pr(\mathbb{I}_\varepsilon = 1) +$$

$$H(\hat{h}_{BA}^K | u_{BA}^K, u_{AB}^K, \mathbb{I}_\varepsilon = 0) \Pr(\mathbb{I}_\varepsilon = 0) + 1 \quad (104)$$

Now consider

$$\begin{aligned} H(\hat{h}_{BA}^K | u_{BA}^K, u_{AB}^K, \mathbb{I}_\varepsilon = 1) &\leq E \left[\log |\mathcal{T}_\varepsilon^K(\hat{h}_{BA} | u_{BA}^K, u_{AB}^K)| \right] \\ &\leq K(H(\hat{h}_{BA} | u_{BA}, u_{AB}) + \gamma_K(\varepsilon)) \end{aligned} \quad (105)$$

where the last step follows from the bound on the size of a conditionally typical set [42, pp. 27].

Furthermore since $\Pr(\mathbb{I}_\varepsilon = 0) \rightarrow 0$ as $K \rightarrow \infty$ we have that (104) simplifies to the following

$$H(\hat{h}_{BA}^K | u_{BA}^K, u_{AB}^K) \leq K \left\{ H(\hat{h}_{BA} | u_{BA}, u_{AB}) + \gamma_K(\varepsilon) \right\} \quad (106)$$

We have the following lower bound on $H(u_{BA}^K, u_{AB}^K)$:

$$H(u_{BA}^K, u_{AB}^K) = H(u_{BA}^K | u_{AB}^K) + H(u_{AB}^K) \quad (107)$$

$$= H(u_{BA}^K, \hat{h}_{BA}^K | u_{AB}^K) - H(\hat{h}_{BA}^K | u_{BA}^K, u_{AB}^K) + H(u_{AB}^K) \quad (108)$$

$$\geq H(\hat{h}_{BA}^K | u_{AB}^K) - H(\hat{h}_{BA}^K | u_{BA}^K, u_{AB}^K) + H(u_{AB}^K) \quad (109)$$

$$\geq K \left\{ I(\hat{h}_{BA}; u_{BA} | u_{AB}) + I(\hat{h}_{AB}; u_{AB}) - \gamma_K(\varepsilon) \right\} \quad (110)$$

¹All the expressions are conditioned on the codebook \mathcal{C} . We suppress this conditioning for sake of convenience.

$$= K \left\{ I(\hat{h}_{BA}; u_{BA}) + I(\hat{h}_{AB}; u_{AB}) - I(u_{BA}; u_{AB}) - 3\gamma_K(\varepsilon) \right\} \quad (111)$$

where we use (102) and (106) in (110).

Now consider

$$H(\bar{\mathbf{v}}_A^K, \bar{\mathbf{v}}_B^K | u_{BA}^K, u_{AB}^K, \bar{\mathbf{z}}^K, \mathbf{g}^K) \geq H(\bar{\mathbf{v}}_A^K, \bar{\mathbf{v}}_B^K | u_{BA}^K, u_{AB}^K, \bar{\mathbf{z}}^K, \mathbf{g}^K, h_{AB}^K, h_{BA}^K) \quad (112)$$

$$= H(\bar{\mathbf{v}}_A^K | h_{BA}^K, \bar{\mathbf{z}}_B^K, \mathbf{g}_{BE}^K) + H(\bar{\mathbf{v}}_B^K | h_{AB}^K, \bar{\mathbf{z}}_A^K, \mathbf{g}_{AE}^K) \quad (113)$$

where (112) follows from the fact that conditioning reduces entropy and (113) follows from the fact that $(\bar{\mathbf{x}}_A^K, \bar{\mathbf{x}}_B^K)$ are generated mutually independently and hence the associated Markov chain holds. We lower bound each of the two terms in (113)

$$\begin{aligned} & H(\bar{\mathbf{v}}_A^K | h_{BA}^K, \bar{\mathbf{z}}_B^K, \mathbf{g}_{BE}^K) \\ &= H(h_{BA}^K, \bar{\mathbf{z}}_B^K, \mathbf{g}_{BE}^K | \bar{\mathbf{v}}_A^K) + H(\bar{\mathbf{v}}_A^K) - H(h_{BA}^K, \bar{\mathbf{z}}_B^K, \mathbf{g}_{BE}^K) \\ &= H(h_{BA}^K, \bar{\mathbf{z}}_B^K, \mathbf{g}_{BE}^K | \bar{\mathbf{v}}_A^K) + H(\bar{\mathbf{v}}_A^K) - KH(h_{BA}, \bar{\mathbf{z}}_B, \mathbf{g}_{BE}) \end{aligned} \quad (114)$$

$$\geq H(h_{BA}^K, \bar{\mathbf{z}}_B^K, \mathbf{g}_{BE}^K | \bar{\mathbf{v}}_A^K) + KI(\bar{\mathbf{v}}_A; \bar{\mathbf{y}}_A) - KH(h_{BA}, \bar{\mathbf{z}}_B, \mathbf{g}_{BE}) - K\gamma_K(\varepsilon) \quad (115)$$

$$\geq K \left\{ H(h_{BA}, \bar{\mathbf{z}}_B, \mathbf{g}_{BE} | \bar{\mathbf{v}}_A) + I(\bar{\mathbf{v}}_A; \bar{\mathbf{y}}_A) - H(h_{BA}, \bar{\mathbf{z}}_B, \mathbf{g}_{BE}) - \gamma_K(\varepsilon) \right\} \quad (116)$$

$$= K \{ I(\bar{\mathbf{v}}_A; \bar{\mathbf{y}}_A) - I(\bar{\mathbf{v}}_A; \bar{\mathbf{z}}_B, h_{BA}, \mathbf{g}_{BE}) - \gamma_K(\varepsilon) \} \quad (117)$$

where (114) follows from the fact that $(h_{AB}^K, \bar{\mathbf{z}}_B^K, \mathbf{g}_{BE}^K)$ are sampled i.i.d. and (115) follows from the fact that $\bar{\mathbf{v}}_A^K$ is distributed nearly uniformly over the set \mathcal{C}_A^K (see e.g., [43, pp. 660, Lemma 1]) and (116) follows from Lemma 1 by substituting $u = \bar{\mathbf{v}}_A$, $y = (h_{BA}, \bar{\mathbf{z}}_B, \mathbf{g}_{BE})$, $x = \mathbf{y}_A$ and $R = I(\bar{\mathbf{y}}_A; \bar{\mathbf{v}}_A) + 2\varepsilon$. In a similar manner we can show that

$$\begin{aligned} & H(\bar{\mathbf{v}}_B^K | h_{AB}^K, \bar{\mathbf{z}}_A^K, \mathbf{g}_{AE}^K) \\ & \geq K \{ I(\bar{\mathbf{v}}_B; \bar{\mathbf{y}}_B) - I(\bar{\mathbf{v}}_B; \bar{\mathbf{z}}_A, h_{AB}, \mathbf{g}_{AE}) - \gamma_K(\varepsilon) \} \end{aligned} \quad (118)$$

Substituting (95)-(98), (111), (117) and (118) into (94) we have established that

$$\begin{aligned} & \frac{1}{K} H(u_{BA}^K, u_{AB}^K, \bar{\mathbf{v}}_A^K, \bar{\mathbf{v}}_B^K | \phi_A, \phi_B, \psi_A, \psi_B, \bar{\mathbf{z}}^K, \mathbf{g}^K) \geq \\ & I(\hat{h}_{AB}; u_{BA}) + I(\hat{h}_{BA}; u_{AB}) - I(u_{BA}; u_{AB}) + \\ & I(\bar{\mathbf{v}}_B; \bar{\mathbf{x}}_A, \mathbf{u}) - I(\bar{\mathbf{v}}_B; h_{AB}, \mathbf{g}_{AE}, \bar{\mathbf{z}}_A) + \\ & I(\bar{\mathbf{v}}_A; \bar{\mathbf{x}}_B, \mathbf{u}) - I(\bar{\mathbf{v}}_A; h_{BA}, \mathbf{g}_{BE}, \bar{\mathbf{z}}_B) - \gamma_K(\varepsilon). \end{aligned} \quad (119)$$

Now observe that

$$\begin{aligned} & I(\bar{\mathbf{v}}_B; \bar{\mathbf{x}}_A, \mathbf{u}) - I(\bar{\mathbf{v}}_B; h_{AB}, \mathbf{g}_{AE}, \bar{\mathbf{z}}_A) \\ &= I(\bar{\mathbf{v}}_B; \bar{\mathbf{x}}_A, \mathbf{u}) - I(\bar{\mathbf{v}}_B; h_{AB}, \mathbf{g}_{AE}, \bar{\mathbf{z}}_A, \mathbf{u}) \end{aligned} \quad (120)$$

$$\begin{aligned} &= H(\bar{\mathbf{v}}_B | h_{AB}, \mathbf{g}_{AE}, \bar{\mathbf{z}}_A, \mathbf{u}) - H(\bar{\mathbf{v}}_B | \bar{\mathbf{x}}_A, \mathbf{u}) \\ &= (T-1) \{ H(v_B | h_{AB}, \mathbf{g}_{AE}, z_A, \mathbf{u}) - H(v_B | x_A, \mathbf{u}) \} \end{aligned} \quad (121)$$

$$\begin{aligned} &= (T-1) \{ I(v_B; x_A, \mathbf{u}) - I(v_B; h_{AB}, \mathbf{g}_{AE}, z_A, \mathbf{u}) \} \\ &= (T-1) \{ I(v_B; x_A, \mathbf{u}) - I(v_B; h_{AB}, \mathbf{g}_{AE}, z_A) \} \end{aligned} \quad (122)$$

where (121) follows from the fact that $\bar{\mathbf{x}}_A \in \mathbb{C}^{T-1}$ is sampled i.i.d. $p_{x_A}(\cdot)$ (120) and (122) follow from the fact that $\mathbf{u} \rightarrow (\bar{\mathbf{z}}_A, \mathbf{g}_{AE}, h_{AB}) \rightarrow \bar{\mathbf{y}}_B \rightarrow \bar{\mathbf{v}}_B$ holds.

In a similar way we can show that

$$\begin{aligned} & I(\bar{\mathbf{v}}_A; \bar{\mathbf{x}}_B, \mathbf{u}) - I(\bar{\mathbf{v}}_A; h_{BA}, \mathbf{g}_{BE}, \bar{\mathbf{z}}_B) \\ &= (T-1) \{ I(v_A; x_B, \mathbf{u}) - I(v_A; h_{AB}, \mathbf{g}_{BE}, z_B) \} \end{aligned} \quad (123)$$

By substituting (122) and (123) into (119) we have that

$$\begin{aligned} & \frac{1}{N} H(u_{BA}^K, u_{AB}^K, \bar{\mathbf{v}}_A^K, \bar{\mathbf{v}}_B^K | \phi_A, \phi_B, \psi_A, \psi_B, \bar{\mathbf{z}}^K, \mathbf{g}^K) \geq \\ & \frac{1}{T} \left\{ I(\hat{h}_{AB}; u_{BA}) + I(\hat{h}_{BA}; u_{AB}) - I(u_{BA}; u_{AB}) \right\} + \\ & \frac{(T-1)}{T} \{ I(v_B; x_A, \mathbf{u}) - I(v_B; h_{AB}, \mathbf{g}_{AE}, z_A) \} + \\ & \frac{(T-1)}{T} \{ I(v_A; x_B, \mathbf{u}) - I(v_A; h_{AB}, \mathbf{g}_{BE}, z_B) \} \gamma_K(\varepsilon) \\ & \triangleq R_{\text{eq}} - \gamma_K(\varepsilon) \end{aligned} \quad (124)$$

G. Secret-Key Generation

It remains to show that a secret-key can be generated at the legitimate terminals that achieves a rate R_{eq} in (124) and satisfies the secrecy constraint.

We consider M i.i.d. repetitions of the coding scheme in the previous section. Let

$$\mathcal{O}^M = (\mathbf{v}_A^{M \cdot K}, \mathbf{v}_B^{M \cdot K}, u_{AB}^{M \cdot K}, u_{BA}^{M \cdot K}) \quad (125)$$

denote the common sequence at the legitimate terminals after M such repetitions. Note that \mathcal{O}^M is sampled i.i.d. from the joint distribution $p(\mathbf{v}_A^K, \mathbf{v}_B^K, u_{AB}^K, u_{BA}^K)$. Similarly let

$$\mathbf{T}^M \triangleq (\phi_A^M, \phi_B^M, \psi_A^M, \psi_B^M, \bar{\mathbf{z}}^{M \cdot K}, \mathbf{g}^{M \cdot K}) \quad (126)$$

denote the observation sequence at the eavesdropper which is also sampled i.i.d. and furthermore from (124) we have that

$$\frac{1}{K} H(\mathcal{O} | \mathbf{T}) \geq R_{\text{eq}} - \gamma_{K, \varepsilon}. \quad (127)$$

Given the common sequence \mathcal{O}^M at the legitimate receivers and the sequence \mathbf{T}^M at the eavesdropper, sampled i.i.d. from a joint distribution, for any rate $R < H(\mathcal{O} | \mathbf{T})$ and $\delta > 0$ there exists a secret-key codebook (see e.g., [42, sec. 22.3.2, pp. 562-563]) such that the secret-key k satisfies

$$\lim_{M \rightarrow \infty} \frac{1}{MK} H(k) \geq (R - \delta), \quad \lim_{M \rightarrow \infty} \frac{1}{MK} I(k; \mathbf{T}^M) \leq \delta.$$

Furthermore for each M , by selecting K sufficiently large, we can make $\gamma_{K, \varepsilon}$ sufficiently small and also guarantee that the error probability in decoding \mathcal{O}^M goes to zero. Thus we can achieve a secret-key rate arbitrarily close to R_{eq} . This completes the proof of our lower bound.

H. Proof of Prop. 2

We evaluate the rate expression in Theorem 3 for jointly Gaussian input distribution. Recall that \hat{h}_{AB} and \hat{h}_{BA} are the MMSE estimates of the channel gains h_{AB} and h_{BA} respectively. Hence we can decompose,

$$h_{AB} = \hat{h}_{AB} + e_{AB}, \quad h_{BA} = \hat{h}_{BA} + e_{BA} \quad (128)$$

where $\hat{h}_{AB} \sim \mathcal{CN}(0, \alpha)$, $\hat{h}_{BA} \sim \mathcal{CN}(0, \alpha)$ are the estimates and $e_{AB} \sim \mathcal{CN}(0, 1 - \alpha)$, $e_{BA} \sim \mathcal{CN}(0, 1 - \alpha)$ are the

estimation errors and where $\alpha = \frac{P_1}{P_1+1}$. For the test channels in (24) we can show the following:

$$I(u_{AB}; \hat{h}_{AB}) = I(u_{BA}; \hat{h}_{BA}) = \log \left(1 + \frac{\alpha}{Q_1} \right) \quad (129)$$

$$I(u_{AB}; \hat{h}_{BA}) = I(u_{BA}; \hat{h}_{AB}) = -\log \left(1 - \frac{\alpha^2 \rho^2}{1 + \frac{Q_1}{\alpha}} \right) \quad (130)$$

$$\begin{aligned} I(u_{AB}; \hat{h}_{AB}) - I(u_{AB}; \hat{h}_{BA}) \\ = \log \left(1 + \frac{\alpha(1 - \alpha^2 \rho^2)}{Q_1} \right) \\ = I(u_{BA}; \hat{h}_{BA}) - I(u_{BA}; \hat{h}_{AB}) \end{aligned} \quad (131)$$

$$I(u_{AB}; u_{BA}) = -\log \left(1 - \frac{\alpha^2 \rho^2}{\left(1 + \frac{Q_1}{\alpha}\right)^2} \right) \quad (132)$$

Substituting in (15), (17) and (18) we have that

$$\begin{aligned} R_I &= \frac{1}{T} \left\{ I(u_{AB}; \hat{h}_{BA}) + I(u_{BA}; \hat{h}_{AB}) - I(u_{AB}; u_{BA}) \right\} \\ &= \frac{1}{T} \left\{ -2 \log \left(1 - \frac{\alpha^2 \rho^2}{1 + \frac{Q_1}{\alpha}} \right) + \log \left(1 - \frac{\alpha^2 \rho^2}{\left(1 + \frac{Q_1}{\alpha}\right)^2} \right) \right\} \end{aligned} \quad (133)$$

where Q_1 is selected to satisfy:

$$\log \left(1 + \frac{\alpha(1 - \alpha^2 \rho^2)}{Q_1} \right) \leq \varepsilon_1(T-1)R_{\text{NC}}(P). \quad (134)$$

We next obtain expression for R_{BA}^- using the test channel (25).

$$R_{\text{BA}}^- = I(v_A; x_B, u_{AB}, u_{BA}) - I(v_A; h_{AB}, z_B, g_{BE}) \quad (135)$$

$$= h(v_A | h_{AB}, z_B, g_{BE}) - h(v_A | u_{AB}, u_{BA}, x_B) \quad (136)$$

we bound each of the two entropy terms as follows.

$$h(v_A | h_{AB}, z_B, g_{BE}) \quad (137)$$

$$= E \left[\log \left(1 + Q_2 + \frac{P_2 |h_{BA}|^2}{1 + P_2 |g_{BE}|^2} \right) \right] + \log(2\pi e) \quad (138)$$

and furthermore

$$\begin{aligned} h(v_A | u_{AB}, u_{BA}, x_B) \\ \leq h(\tilde{h}_{BA} x_B + q_{BA} + n_{BA}) \end{aligned} \quad (139)$$

$$\leq \log(\sigma_{AB}^2 P_2 + Q_2 + 1) + \log(2\pi e). \quad (140)$$

where

$$\tilde{h}_{BA} = h_{BA} - \hat{h}_{BA}$$

is the error in the MMSE estimate of h_{BA} given (u_{AB}, u_{BA}) and σ_{AB}^2 is the associated estimation error

$$\sigma_{AB}^2 = E[(h_{AB} - \hat{h}_{AB})^2] \quad (141)$$

The upper bound in (140) follows from the fact that a Gaussian input maximizes the differential entropy for a given noise variance. The expression in (30) follows by substituting (138) and (140) into (136). In a similar way we can establish (31).

The rate constraint in (22) and (23) follow by substituting (25) into

$$I(v_A; y_A | x_A, u_{AB}, u_{BA}) \leq \varepsilon_2 R_{\text{NC}}(P). \quad (142)$$

Note that

$$\begin{aligned} I(v_A; y_A | x_A, u_{AB}, u_{BA}) \\ = h(v_A | x_A, u_{AB}, u_{BA}) - h(q_{BA}) \end{aligned} \quad (143)$$

$$\leq \log \left(1 + \frac{\sigma_{AB}^2 P_2 + 1}{Q_1} \right). \quad (144)$$

The expression (33) follows from (142) and (144).

Finally the bound on σ_{AB}^2 in (32) is obtained as follows

$$\begin{aligned} \sigma_{AB}^2 &= E[(h_{AB} - \hat{h}_{AB}(u_{AB}, u_{BA}))^2] \\ &\leq E[(h_{AB} - \hat{h}_{AB}(u_{AB}))^2] \leq 1 - \frac{\alpha^2}{Q_1 + \alpha} \end{aligned} \quad (145)$$

This completes the proof of Prop. 2.

VI. PROOF OF COROLLARY 1

We establish (35) and (36) respectively.

We consider the expression for R^+ in Theorem 1 and show that

$$\lim_{P \rightarrow \infty} R^+ = -\frac{1}{T} \log(1 - \rho^2) + \gamma \quad (146)$$

where γ is defined in (37). In particular note that the first term in (3) is independent of P and furthermore since h_{AB} and h_{BA} are jointly Gaussian, zero mean, unit variance and with a cross-correlation of ρ it can be readily shown that

$$I(h_{AB}; h_{BA}) = -\log(1 - \rho^2). \quad (147)$$

Only the second and third terms depend on P . For any power allocation $P(h_{AB})$ note that

$$E \left[\log \left(1 + \frac{P(h_{AB}) |h_{AB}|^2}{1 + P(h_{AB}) |g_{AE}|^2} \right) \right] \leq E \left[\log \left(1 + \frac{|h_{AB}|^2}{|g_{AE}|^2} \right) \right] \quad (148)$$

which follows since the function $f(x) = \frac{ax}{1+bx}$ is increasing in x for any $a, b > 0$. Similarly we have

$$E \left[\log \left(1 + \frac{P(h_{BA}) |h_{BA}|^2}{1 + P(h_{BA}) |g_{BE}|^2} \right) \right] \leq E \left[\log \left(1 + \frac{|h_{BA}|^2}{|g_{BE}|^2} \right) \right]. \quad (149)$$

Furthermore since a Gaussian input distribution maximizes the conditional mutual information (c.f. (55)), the upper bound follows by substituting (148) and (149) into (3).

We next show that,

$$\lim_{P \rightarrow \infty} R_{\text{PD}}^- = -\frac{1}{T} \log(1 - \rho^2) + \frac{T-1}{T} \gamma. \quad (150)$$

In particular we consider the secret-key rate expression (10) in Prop. 1. We select $P_2 = \frac{\sqrt{P}}{T-1}$ and $P_1 = P - \sqrt{P}$. Note that as $P \rightarrow \infty$ we have that $P_1, P_2 \rightarrow \infty$ and $\frac{P_2}{P_1} \rightarrow 0$. In particular, since $\alpha = \frac{P_1}{P_1+1}$ we have that

$$\lim_{P \rightarrow \infty} -\log(1 - \alpha^2 \rho^2) = -\log(1 - \rho^2), \quad (151)$$

$$\lim_{P \rightarrow \infty} \log \left(1 + \frac{P_2}{1 + P_1} \right) = 0. \quad (152)$$

Furthermore since the function $f(x) = \frac{ax}{1+bx}$ is bounded for all $a, b > 0$ we can apply the Dominated Convergence Theorem,

$$\lim_{P_2 \rightarrow \infty} E \left[\log \left(1 + \frac{P_2 |h_{AB}|^2}{1 + P_2 |g_{AE}|^2} \right) \right] = E \left[\log \left(1 + \frac{|h_{AB}|^2}{|g_{AE}|^2} \right) \right] \quad (153)$$

$$\lim_{P_2 \rightarrow \infty} E \left[\log \left(1 + \frac{P_2 |h_{BA}|^2}{1 + P_2 |g_{BE}|^2} \right) \right] = E \left[\log \left(1 + \frac{|h_{BA}|^2}{|g_{BE}|^2} \right) \right] \quad (154)$$

Substituting (151), (152), (153), (154) into (10), (11), (12), (13) we recover (150). Comparing (150) and (146) we establish (35).

To establish (36) we consider (26) in Prop. 2 and show that with a suitable choice of Q_1 , Q_2 , P_1 and P_2 we have that

$$\lim_{P \rightarrow \infty} R^- = -\frac{1}{T} \log(1 - \rho^2) + \frac{T-1}{T} \gamma. \quad (155)$$

In particular we select $P_2 = \frac{\sqrt{P}}{T-1}$ and $P_1 = P - \sqrt{P}$. Furthermore we select

$$Q_1 = \frac{\alpha(1 - \alpha^2 \rho^2)}{\varepsilon_1(T-1)R_{\text{NC}}(P)} \quad (156)$$

$$Q_2 = \frac{\sigma_{AB}^2 P_2 + 1}{\varepsilon_2 R_{\text{NC}}(P)} \quad (157)$$

Note that as $P \rightarrow \infty$, it is well known that $R_{\text{NC}}(P) \rightarrow \infty$. Thus we can let ε_1 and ε_2 to be any functions of P such that $\varepsilon_1(P), \varepsilon_2(P) \rightarrow 0$ and $\varepsilon_i(P)R_{\text{NC}}(P) \rightarrow \infty$. Then observe that $Q_1, Q_2 \rightarrow 0$ as $P \rightarrow \infty$. It therefore follows that

$$\lim_{P \rightarrow \infty} R_I(\varepsilon_1, P) = -\frac{1}{T} \log(1 - \rho^2), \quad (158)$$

$$\lim_{P \rightarrow \infty} \log \left(1 + \frac{\sigma_{AB}^2 P_2}{1 + Q_2} \right) = 0. \quad (159)$$

and hence we have

$$\lim_{P \rightarrow \infty} R_{\text{AB}}^- = E \left[\log \left(1 + \frac{|h_{AB}|^2}{|g_{AE}|^2} \right) \right] \quad (160)$$

$$\lim_{P \rightarrow \infty} R_{\text{BA}}^- = E \left[\log \left(1 + \frac{|h_{BA}|^2}{|g_{BE}|^2} \right) \right] \quad (161)$$

By substituting (158), (160) and (161) into (26) we obtain (155).

VII. CONCLUSION

We study secret-key agreement capacity over a two-way, non-coherent, reciprocal, block-fading channel. Our main observation is that a separation based scheme that judiciously combines channel-training and randomness-sharing techniques is an efficient approach when the coherence block length is large and the high signal-to-noise is high. Numerical results indicate that even when the overhead of transmitting public messages is accounted for, the proposed scheme outperforms a idealized training-only schemes for moderate SNR and relatively small coherence block-lengths. These observations suggest that when the channel fluctuations are relatively slow, one should not rely on channel reciprocity alone for secret-key generation. We also establish an upper bound on the secret-key agreement capacity and show that the upper and lower bounds coincide asymptotically.

In terms of future work a number of interesting directions remain to be explored. The secret-key agreement capacity in the low signal to noise ratio regime remains to be studied. Potentially improved upper and lower bounds for moderate SNR may be also obtained. While our upper bound and lower bounds naturally extend to the case of multiple antennas a detailed analysis is left for future work. We note that some preliminary investigation along these lines has appeared in [44].

APPENDIX A PROOF OF LEMMA 1

We lower bound the conditional entropy term as follows

$$H(y^n | u^n(L)) = H(y^n, x^n | u^n(L)) - H(x^n | y^n, u^n(L)) \quad (162)$$

$$\geq H(y^n, x^n) - H(u^n(L)) - H(x^n | y^n, u^n(L)) \quad (163)$$

$$= nH(y, x) - H(u^n(L)) - H(x^n | y^n, u^n(L)) \quad (164)$$

$$\geq nH(y, x) - nR - H(x^n | y^n, u^n(L)) \quad (165)$$

where (164) follows from the fact that (x^n, y^n) are sampled independently of \mathcal{A} and (165) follows from the fact that $|\mathcal{A}| = 2^{nR}$. It only remains to upper bound the conditional entropy term in (165). Let $\mathbb{I}_{\varepsilon'}$ denote an indicator function that equals 1 if $(x^n, y^n, u^n) \in T_{\varepsilon'}^n(x, y, u)$ and equals zero otherwise. From the conditional typicality lemma we have that $\Pr(\mathbb{I}_{\varepsilon'} = 1) \rightarrow 1$ as $n \rightarrow \infty$, for any $\varepsilon' > \varepsilon$.

$$H(x^n | y^n, u^n(L)) \leq 1 + H(x^n | y^n, u^n(L), \mathbb{I}) \quad (166)$$

$$= 1 + H(x^n | y^n, u^n(L), \mathbb{I} = 1) \Pr(\mathbb{I} = 1) + H(x^n | y^n, u^n(L), \mathbb{I} = 0) \Pr(\mathbb{I} = 0) \quad (167)$$

$$\leq 1 + H(x^n | y^n, u^n(L), \mathbb{I} = 1) + nH(x) \Pr(\mathbb{I} = 0) \quad (168)$$

$$\leq 1 + E[\log |\mathcal{T}_{\varepsilon'}^n(x | u^n, y^n)|] + nH(x) \Pr(\mathbb{I} = 0) \quad (169)$$

$$\leq 1 + nH(x | u, y) + n\gamma(\varepsilon) + n\gamma_n(\varepsilon) \quad (170)$$

where we use the fact that for any $\varepsilon > 0$, $\Pr(\mathbb{I} = 0) \rightarrow 0$ as $n \rightarrow \infty$ in (168), which follows since $R > I(x; u)$. Combining (165) and (170) we get

$$H(y^n | u^n(L)) \geq n \{ H(y, x) - H(x | y, u) - R - \gamma_n(\varepsilon) \} \quad (171)$$

$$= n \{ H(y | x) + H(x) - H(x | u) + I(x; y | u) - R - \gamma_n(\varepsilon) \} \quad (172)$$

$$= n \{ H(y | u) + I(x; u) - R - \gamma_n(\varepsilon) \}, \quad (173)$$

where the last step uses the fact that $u \rightarrow x \rightarrow y$.

REFERENCES

- [1] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Information Forensics and Security*, vol. 3, no. 2, pp. 364–375, 2007.
- [2] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. B. Mandayam, "Exploiting the physical layer for enhanced security," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 63–70, 2010.
- [3] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

- [4] J. Croft, "Shared secret key establishment using wireless channel measurements," Ph.D. dissertation, University of Utah, 2011.
- [5] M. Ko, "Wireless physical-layer security performance of UWB systems," Master's thesis, UMass Amherst, 2011.
- [6] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, no. 2, pp. 207–212, 1996.
- [7] N. Patwari, J. Croft, S. Jana, and S. K. Kasper, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mob. Comput.*, vol. 9, no. 1, pp. 17–30, 2010.
- [8] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *14th ACM conference on Computer and communications security*, 2007, pp. 401–410.
- [9] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.
- [10] M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of generating a secret key using wireless fading under active adversary," *IEEE/ACM Trans. Netw.*, vol. 20, no. 5, pp. 1440–1451, 2012.
- [11] S. Vasudevan, D. Goeckel, and D. F. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *MobiHoc*, 2010, pp. 21–30.
- [12] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation," in *INFOCOM*, 2011, pp. 2165–2173.
- [13] K. Zeng, D. Wu, A. J. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *INFOCOM*, 2010, pp. 1837–1845.
- [14] J. Zhang, S. K. Kasper, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in *INFOCOM*, 2010, pp. 261–265.
- [15] M. G. Madiseh, S. W. Neville, and M. L. McGuire, "Applying beamforming to address temporal correlation in wireless channel characterization-based secret key generation," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1278–1287, 2012.
- [16] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *INFOCOM*, 2011, pp. 1422–1430.
- [17] B. Hamida, J.-B. Pierrot, and C. Castelluccia, "An adaptive quantization algorithm for secret key generation using radio channel measurements," in *NTMS*, 2009, pp. 1–5.
- [18] T. Shimizu, N. Otani, T. Kitano, H. Iwai, and H. Sasaoka, "Experimental validation of wireless secret key agreement using array antennas," in *URSI General Assembly and Scientific Symposium*, 2011, pp. 1–5.
- [19] M. G. Madiseh, "Wireless secret key generation versus capable adversaries," Ph.D. dissertation, University of Victoria, 2011.
- [20] J. W. Wallace and R. K. Sharma, "Experimental investigation of MIMO reciprocal channel key generation," in *ICC*, 2010, pp. 1–5.
- [21] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.
- [22] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 2, pp. 480–490, Apr. 2012.
- [23] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, Mar. 1993.
- [24] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography – Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121–1132, July 1993.
- [25] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, 2004.
- [26] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals - part I: Source model," *IEEE Trans. Inform. Theory*, vol. 56, no. 8, pp. 3973–3996, 2010.
- [27] —, "Information-theoretic key agreement of multiple terminals - part II: Channel model," *IEEE Trans. Inform. Theory*, vol. 56, no. 8, pp. 3997–4010, 2010.
- [28] V. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via sources and channels," *IEEE Trans. Inform. Theory*, submitted, Nov. 2009. [Online]. Available: <http://www.ifp.illinois.edu/~vinodmp/publications/Secrecy09.pdf>
- [29] S. Haile, "Investigation of channel reciprocity for OFDM TDD systems," Master's thesis, U. Waterloo, 2009.
- [30] F. Kaltenberger, H. Jiang, M. Guillaud, and R. Knopp, "Relative channel reciprocity calibration in MIMO/TDD systems," in *Future Netw. Mobile Summit*, 2010.
- [31] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.
- [32] A. Agrawal, Z. Rezki, A. Khisti, and M. S. Alouini, "Noncoherent secret-key agreement with public discussion," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 3, pp. 565–574, 2011.
- [33] Y. Abdallah, M. A. Latif, M. Youssef, A. Sultan, and H. E. Gamal, "Keys through arq: Theory and practice," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3-1, pp. 737–751, 2011.
- [34] O. O. Koyluoglu and H. E. Gamal, "Polar coding for secure transmission and key agreement," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1472–1483, 2012.
- [35] M. A. Latif, A. Sultan, and H. E. Gamal, "Arq-based secret key sharing," in *ICC*, 2009, pp. 1–6.
- [36] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "A broadcast approach to secret key generation over slow fading channels," *CoRR*, vol. abs/1103.3113, 2011.
- [37] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key agreement with channel state information at the transmitter," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 3, 2011.
- [38] A. Khisti and S. N. Diggavi, "A remark on secret-key generation over correlated fading channels," in *Globecom, Workshop on Physical Layer Security*, Houston, TX, 2011.
- [39] A. Khisti, "Secret-key agreement over wiretap channels with transmitter side information," in *European Wireless*, Lucca, Italy, Apr. 2010.
- [40] B. Hassibi and B. M. Hochwald, "How much training is needed in a multiple-antenna wireless link?" *IEEE Trans. Inform. Theory*, Apr. 2011.
- [41] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, 2009.
- [42] A. E. Gamal and Y. H. Kim, *Network Information Theory*. Cambridge, UK: Cambridge University Press, 2012.
- [43] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key generation using correlated sources and channels," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 652–670, 2012.
- [44] M. Andersson, A. Khisti, and M. Skoglund, "Secret-key agreement over a non-coherent block-fading MIMO wiretap channel," in *IEEE ITW*, Lausanne, Switzerland, 2012, pp. 53–57.